@ΣΗΔΕ ΙΡΙΔΑ
6819eb72553adfe7ddb033cc
ΑΠ:25284
Υπογραφή: 09/05/25 13:18
Διανομή: 09/05/25 16:18

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΟΙΚΟΝΟΜΙΚΩΝ ΥΠΗΡΕΣΙΩΝ
& ΔΙΟΙΚΗΤΙΚΗΣ ΥΠΟΣΤΗΡΙΞΗΣ
ΔΙΕΥΘΥΝΣΗ ΠΡΟΜΗΘΕΙΩΝ & ΥΠΟΔΟΜΩΝ ΤΜΗΜΑ ΠΡΟΜΗΘΕΙΩΝ
Πληροφορίες: Χρυσούλα Γιατρά
Ταχ. Δ/νση: Σταδίου 31
Ταχ. Κώδικας: 101 83
Τηλέφωνο: 213 136 1731
email: ch.giatra@ypes.gr

Αθήνα, 09-05-2025
Αρ. Πρωτ.: 25284

ΠΡΟΣ ΤΟΝ ΟΙΚΟΝΟΜΙΚΟ ΦΟΡΕΑ: MODUS A.E.

email: sales@modus.gr

ΘΕΜΑ: Πρόσκληση κατάθεσης οικονομικής προσφοράς για την παροχή υπηρεσιών ανάπτυξης νέου Ολοκληρωμένου Πληροφοριακού Σύστηματος (ΟΠΣ) Ψηφιακής Προ-έγκρισης Αιτημάτων Ληξιαρχικών Μητρώων

Το Υπουργείο Εσωτερικών, προκειμένου να καλυφθεί η ανάγκη για την παροχή υπηρεσιών ανάπτυξης νέου Ολοκληρωμένου Πληροφοριακού Σύστηματος (ΟΠΣ) Ψηφιακής Προ-έγκρισης Αιτημάτων Ληξιαρχικών Μητρώων θα προβεί στη σύναψη σχετικής σύμβασης.

Κατόπιν έκδοσης της υπ. αριθμ. πρωτ. 13805/29-04-2025 διαπιστωτικής πράξης από το Υπουργείο Ψηφιακής Διακυβέρνησης που καθιστά επιτρεπτή την κατά παρέκκλιση της παρ.1 του άρθρου 4412/2016 προσφυγή στη διαδικασία της απευθείας ανάθεσης για έργα Τεχνολογιών Πληροφοριών και Επικοινωνιών (Τ.Π.Ε) , θα ακολουθηθεί η διαδικασία του ν.4412/2016 (Α’ 147) «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)», όπως έχει τροποποιηθεί και ισχύει, και ιδίως των διατάξεων περί απευθείας ανάθεσης του άρθρου 118 και πιο συγκεκριμένα της παρ.6 για αναθέσεις συμβάσεων προμηθειών, υπηρεσιών, έργων και μελετών και τεχνικών και λοιπών συναφών επιστημονικών υπηρεσιών, που αφορούν στην υλοποίηση έργων ΤΠΕ με αντικείμενο την εξασφάλιση της διαλειτουργικότητας των ψηφιακών υπηρεσιών ή τον εκσυγχρονισμό των ψηφιακών εργαλείων της Κεντρικής Διοίκησης κατά την έννοια της περ. στ’ της παρ. 1 του άρθρου 14 του ν. 4270/2014 (Α’ 143) και της παρ. 3 του άρθρου 120.

Ο προσκαλούμενος οικονομικός φορέας καλείται να καταθέσει την προσφορά του βάσει των ειδικών τεχνικών όρων και των προδιαγραφών των παρακάτω παραρτημάτων τα οποία αποτελούν **αναπόσπαστο μέρος** της παρούσας πρόσκλησης.

- Παράρτημα 1: Γενικά Στοιχεία Πρόσκλησης
- Παράρτημα 2: Τεχνικές Προδιαγραφές
- Παράρτημα 3: Κατάρτιση Προσφοράς
- Παράρτημα 4: Οικονομικά Στοιχεία του Έργου – Τρόπος πληρωμής
- Παράρτημα 5: Προστασία προσωπικών δεδομένων - Υποχρέωση εχεμύθειας και εμπιστευτικότητας

Ο ΥΠΗΡΕΣΙΑΚΟΣ ΓΡΑΜΜΑΤΕΑΣ

ΠΑΝΤΕΛΗΣ ΤΑΓΚΑΛΑΚΗΣ

<u>Εσωτερική Διανομή</u>:

1. Γραφείο Γενικού Γραμματέα Εσωτερικών και Οργάνωσης
2. Γραφείο Υπηρεσιακού Γραμματέα
3. Διεύθυνση Ηλεκτρονικής Διακυβέρνησης
4. Διεύθυνση Προμηθειών & Υποδομών
5. Υπεύθυνος Επεξεργασίας Προσωπικών Δεδομένων

ΠΑΡΑΡΤΗΜΑ 1

Γενικά Στοιχεία Πρόσκλησης

ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ	ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ (Τ. Εσωτερικών)
ΜΟΝΑΔΑ ΦΟΡΕΑ	ΔΙΕΥΘΥΝΣΗ ΠΡΟΜΗΘΕΙΩΝ ΚΑΙ ΥΠΟΔΟΜΩΝ ΤΜΗΜΑ ΠΡΟΜΗΘΕΙΩΝ
ΕΙΔΟΣ ΣΥΜΒΑΣΗΣ	Απευθείας ανάθεση βάσει της παρ.6 του άρθρου 118 και της παρ.3 του άρθρου 120 του ν.4412/2016, όπως έχει τροποποιηθεί και ισχύει, κατόπιν της έκδοσης της υπ. αριθμ. πρωτ. 13805/29-04-2025 διαπιστωτικής πράξης από το Υπουργείο Ψηφιακής Διακυβέρνησης που καθιστά επιτρεπτή την κατά παρέκκλιση της παρ.1 του άρθρου 4412/2016 προσφυγή στη διαδικασία της απευθείας ανάθεσης για έργα Τεχνολογιών Πληροφοριών και Επικοινωνιών (Τ.Π.Ε).
ΠΕΡΙΓΡΑΦΗ ΘΕΜΑΤΟΣ	Παροχή υπηρεσιών ανάπτυξης νέου Ολοκληρωμένου Πληροφοριακού Σύστηματος (ΟΠΣ) Ψηφιακής Προ-έγκρισης Αιτημάτων Ληξιαρχικών Μητρώων. Οι προδιαγραφές των ανωτέρω υπηρεσιών αναφέρονται στα Παραρτήματα 1, 2, 3, 4, και 5 τα οποία αποτελούν αναπόσπαστο μέρος της παρούσας **(ΕΠΙ ΠΟΙΝΗ ΑΠΟΚΛΕΙΣΜΟΥ)**.
ΠΡΟΣΚΑΛΟΥΜΕΝΟΣ ΟΙΚΟΝΟΜΙΚΟΣ ΦΟΡΕΑΣ	Για τη σύναψη της σχετικής σύμβασης, το Υπουργείο Εσωτερικών προσκαλεί την ενδιαφερόμενη εταιρεία να καταθέσει οικονομική και τεχνική προσφορά βάσει των ειδικών τεχνικών όρων και των προδιαγραφών του παρακάτω παραρτήματος το οποίο αποτελεί αναπόσπαστο μέρος της παρούσας πρόσκλησης. **(ΕΠΙ ΠΟΙΝΗ ΑΠΟΚΛΕΙΣΜΟΥ)** Η προσφορά υποβάλλεται για το σύνολο των υπηρεσιών, επί ποινή αποκλεισμού. **Δε λαμβάνονται υπόψη προσφορές οικονομικών φορέων που δεν προσκλήθηκαν να υποβάλουν προσφορά, σύμφωνα με τις διατάξεις του άρθρου 120 παρ. 3 του ν.4412/2016, όπως ισχύει.**
ΕΚΤΙΜΩΜΕΝΟ ΚΟΣΤΟΣ	**Ποσό άνευ Φ.Π.Α. :** 60.000,00€ **Ποσό συμπεριλαμβανομένου Φ.Π.Α. :** 74.400,00€
ΚΩΔΙΚΟΣ ΠΡΟΫΠΟΛΟΓΙΣΜΟΥ ΦΟΡΕΑ	Τακτικός Προϋπολογισμός , Ειδικός Φορέας 1007-206 ΑΛΕ 2420989001

ΠΑΡΑΚΡΑΤΗΣΗ ΦΟΡΟΥ ΕΠΙ ΤΗΣ ΚΑΘΑΡΗΣ ΣΥΜΒΑΤΙΚΗΣ ΑΞΙΑΣ	**Φόρος**: 8% (οκτώ τοις εκατό) για την παροχή υπηρεσιών σύμφωνα με το άρθρο 64 του ν.4172/2013, όπως τροποποιήθηκε και ισχύει. **Κρατήσεις:** 0,1% υπέρ της Ενιαίας Αρχής Δημόσιων Συμβάσεων (ΕΑΔΗΣΥ). Η κράτηση αυτή υπολογίζεται επί της αξίας κάθε πληρωμής προ φόρων και κρατήσεων της αρχικής, καθώς και κάθε συμπληρωματικής ή τροποποιητικής σύμβασης, σύμφωνα με το άρθρο 350 του Ν.4412/2016, όπως αντικαταστάθηκε με το άρθρο 7 Ν.4912/2022 (Α' 59) (Σχ. και άρθρο 17 του ίδιου νόμου και Ανακοίνωση 24.10.2022 της ΕΑΔΗΣΥ).
ΤΕΚΜΗΡΙΩΜΕΝΟ ΑΙΤΗΜΑ - ΑΠΟΦΑΣΗ ΑΝΑΛΗΨΗΣ ΥΠΟΧΡΕΩΣΗΣ	Υπ' αρ. 13689/13-03-2025 (ΑΔΑΜ: 25REQ016582570) Υπ' αρ. 16876/27-03-2025 (ΑΔΑΜ: 25REQ016582717)
ΚΑΤΑΛΗΚΤΙΚΗ ΠΡΟΘΕΣΜΙΑ ΚΑΤΑΘΕΣΗΣ ΠΡΟΣΦΟΡΑΣ	Εως την **Πέμπτη 15 Μαΐου 2025** και **ώρα 12:00** σε κλειστό σφραγισμένο φάκελο. Προσφορά που θα υποβληθεί μετά το πέρας της προαναφερόμενης ημερομηνίας και ώρας θεωρείται **ΕΚΠΡΟΘΕΣΜΗ** και δε λαμβάνεται υπόψη. Η ισχύς της προσφοράς θα πρέπει να είναι οι 30 ημέρες.
ΤΑΧ. ΔΙΕΥΘΥΝΣΗ ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ ΚΑΙ ΤΟΠΟΣ ΚΑΤΑΘΕΣΗΣ ΠΡΟΣΦΟΡΑΣ	Υπουργείο Εσωτερικών Δ/νση Προμηθειών & Υποδομών Τμήμα Προμηθειών Υπόψη Χ. Γιατρά Σταδίου 31, 4ος όροφος, Τ.Κ. 101 83 Αθήνα Τηλέφωνο επικοινωνίας : 213 136 1731
ΕΓΓΥΗΤΙΚΗ ΕΠΙΣΤΟΛΗ ΚΑΛΗΣ ΕΚΤΕΛΕΣΗΣ	Εντός πέντε (5) ημερών από την υπογραφή της απόφασης ανάθεσης ο Ανάδοχος θα πρέπει να καταθέσει εγγυητική επιστολή καλής εκτέλεσης σύμφωνα με την παρ. 4 του άρ. 72 του ν. 4412/16, σε ποσοστό 4% επί του τελικού συμβατικού τιμήματος χωρίς το Φ.Π.Α.. **Σε περίπτωση που δεν προσκομιστεί η εν λόγω εγγυητική επιστολή, η σύμβαση λύεται αυτοδίκαια και δεν καταβάλλεται στον ανάδοχο καμία αμοιβή για τις ήδη παρεχόμενες υπηρεσίες**
ΤΡΟΠΟΣ ΤΙΜΟΛΟΓΗΣΗΣ	Απαιτείται η έκδοση **ηλεκτρονικού τιμολογίου** (ΗΤ) κατά τα οριζόμενα στον ν.4601/2019 και στις ΚΥΑ αριθμ. 13005/01.02.2022 (Β' 438), 98979/10.08.2021 (Β' 3766), 63446/31-05-2021 (Β' 2338) και ΚΥΑ 52445 ΕΞ 2023 (Β' 2385). Διευκρινίζεται ότι παράλληλα ισχύουν και οι διατάξεις των ΥΑ αριθμ. Α.1035/18-02-2020 (Β' 551) και Α.1138/12-06-2020 (Β' 2470), στις οποίες μεταξύ άλλων προβλέπεται η χρήση παρόχων υπηρεσιών ηλεκτρονικής έκδοσης στοιχείων. Περισσότερες

	πληροφορίες μπορείτε να βρείτε στο https: www.gsis.gr/polites-epiheiriseis/pliromes-kai-eispraxeis/e-invoice
ΣΤΟΙΧΕΙΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΙΜΟΛΟΓΗΣΗΣ ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ:	ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ ΑΦΜ: 090056250 ΔΟΥ: ΚΕΦΟΔΕ ΑΤΤΙΚΗΣ ΚΩΔΙΚΟΣ ΑΑΗΤ: 1007.0000000000.0001 ΑΔΑ ΑΠΟΦΑΣΗΣ ΑΝΑΛΗΨΗΣ ΥΠΟΧΡΕΩΣΗΣ: 9Λ7246ΜΤΛ6-7ΓΗ
ΚΑΝΟΝΕΣ ΔΗΜΟΣΙΟΤΗΤΑΣ:	Η παρούσα ανακοίνωση αναρτάται: α) στην ιστοσελίδα του ΥΠΕΣ www.ypes.gr β) στο Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ) www.eprocurement.gov.gr

ΠΑΡΑΡΤΗΜΑ 2

Τεχνικές Προδιαγραφές

2.1 Περιγραφή Υφιστάμενης Κατάστασης

Η διαδικασία εγγραφής ληξιαρχικών πράξεων που έχουν εκδοθεί σε τρίτες χώρες πραγματοποιείται μέσω της φυσικής προσέλευσης των ενδιαφερόμενων πολιτών ή των πληρεξουσίων δικηγόρων τους στο Ειδικό Ληξιαρχείο, όπου υποβάλλονται τα απαιτούμενα έγγραφα (ληξιαρχικές πράξεις και σχετικές μεταφράσεις με ή χωρίς Apostille).

Σημαντικές δυσχέρειες προκύπτουν κατά την υλοποίηση της διαδικασίας, καθώς, παρά τις πολύωρες αναμονές, ένα ποσοστό των υποβληθέντων δικαιολογητικών απορρίπτεται ως μη έγκυρο, με αποτέλεσμα οι ενδιαφερόμενοι να υποχρεώνονται να επανέλθουν με διορθωμένα ή συμπληρωματικά έγγραφα και να επαναλάβουν τη διαδικασία από την αρχή. Αυτή η επαναλαμβανόμενη και χρονοβόρα διαδικασία συνεπάγεται επιπλέον διοικητική επιβάρυνση, δυσχεραίνει την εξυπηρέτηση των πολιτών και προκαλεί σημαντική ταλαιπωρία στους ενδιαφερόμενους και στους πληρεξούσιους δικηγόρους τους.

2.2 Περιγραφή Φυσικού Αντικειμένου

Προκειμένου να βελτιωθεί η αποδοτικότητα της διαδικασίας και να ελαχιστοποιηθεί η ανάγκη πολλαπλών φυσικών επισκέψεων, θα υλοποιηθεί Ολοκληρωμένο Σύστημα Ψηφιακής Προ-έγκρισης Αιτημάτων Ληξιαρχικών Μητρώων. Το σύστημα θα δίνει την δυνατότητα στους πολίτες και στους πληρεξούσιους δικηγόρους τους να

υποβάλλουν ψηφιακά αντίγραφα των πρωτότυπων για εγγραφή στα ληξιαρχικά μητρώα (Γέννησης, Γάμου, Λύσης Γάμου, Θανάτου), ώστε στη συνέχεια οι αρμόδιοι χειριστές του ληξιαρχείου να πραγματοποιούν προκαταρκτικό έλεγχο εγκυρότητας και πληρότητας. Μόνο κατόπιν θετικής προέγκρισης, οι ενδιαφερόμενοι θα προσέρχονται για την υποβολή των πρωτότυπων εγγράφων, διασφαλίζοντας την οριστική καταχώριση του αιτήματος, σύμφωνα με το ισχύον θεσμικό πλαίσιο.

Η λύση αναμένεται να συμβάλει καθοριστικά στην επιτάχυνση των διαδικασιών, στη μείωση της διοικητικής επιβάρυνσης, στη βελτίωση της εμπειρίας των πολιτών και των πληρεξούσιων δικηγόρων τους, καθώς και στην ενίσχυση της επιχειρησιακής αποδοτικότητας των αρμόδιων υπηρεσιών.

2.3 Υλοποίηση Συστήματος Ψηφιακής Προ-έγκρισης Αιτημάτων Ληξιαρχικών Μητρώων

Το Ολοκληρωμένο Σύστημα Ψηφιακής Προ-έγκρισης Αιτημάτων Ληξιαρχικών Μητρώων θα σχεδιαστεί με σκοπό τη βελτιστοποίηση της διαδικασίας εγγραφής ληξιαρχικών πράξεων από τρίτες χώρες, εξασφαλίζοντας την αποτελεσματικότητα, τη διαφάνεια και την ασφάλεια των σχετικών διαδικασιών.

Το σύστημα θα παρέχει στους ενδιαφερόμενους πολίτες και στους πληρεξούσιους δικηγόρους τους τη δυνατότητα ηλεκτρονικής υποβολής αιτήσεων και εγγράφων σε ψηφιακή μορφή, διευκολύνοντας την αρχική αξιολόγηση της εγκυρότητας των στοιχείων πριν την υποχρεωτική φυσική προσέλευση. Με αυτόν τον τρόπο, θα περιοριστούν οι επαναλαμβανόμενες επισκέψεις στο Ειδικό Ληξιαρχείο, μειώνοντας τον χρόνο διεκπεραίωσης των αιτημάτων και βελτιώνοντας την εμπειρία εξυπηρέτησης των πολιτών.

Το σύγχρονο διαδικτυακό περιβάλλον που θα αναπτυχθεί θα είναι φιλικό προς τον χρήστη και πλήρως προσβάσιμο από κινητές συσκευές. Το σύστημα θα απευθύνεται σε πολίτες και δικηγόρους και θα επιτρέπει την υποβολή των εκάστοτε αιτημάτων με δυνατότητα επισύναψης των απαραίτητων δικαιολογητικών καθώς και την αυτοματοποιημένη ενημέρωση για την πορεία και το ιστορικό της διαδικασίας προ-έγκρισης κάθε αιτήματος.

- Το σύστημα ψηφιακής προ-έγκρισης αιτημάτων ληξιαρχικών μητρώων θα φιλοξενηθεί στο G-Cloud, διασφαλίζοντας υψηλή διαθεσιμότητα, ασφάλεια και κλιμάκωση.
- Διαδικτυακή πρόσβαση και αυθεντικοποίηση χρηστών
  - Το ολοκληρωμένο σύστημα ψηφιακής προ-έγκρισης αιτημάτων ληξιαρχικών μητρώων θα παρέχει διαδικτυακή πρόσβαση στους πολίτες και στους πληρεξούσιους δικηγόρους μέσω υπολογιστών, κινητών συσκευών ή/και ταμπλετών.
  - Η αυθεντικοποίηση των χρηστών στο σύστημα θα γίνεται:
    a) Για τους ενδιαφερόμενους πολίτες, μέσω του Taxisnet
    b) Για τους ενδιαφερόμενους πολίτες που δεν διαθέτουν πρόσβαση στο TaxisNet, θα παρέχεται εναλλακτική μέθοδος ταυτοποίησης μέσω email και κινητού τηλεφώνου, με την αποστολή κωδικού OTP (One-Time Password).
    c) Για τους πληρεξούσιους δικηγόρους, μέσω του μητρώου δικηγόρων (https://www.olomeleia.gr/)
- Υποβολή και Διαχείριση Αιτημάτων
  - Η υποβολή των ψηφιακών αιτημάτων θα γίνεται με καταχώριση των απαιτούμενων στοιχείων και την ψηφιακή μεταφόρτωση των σχετικών συνοδευτικών εγγράφων.

- Με την υποβολή του ψηφιακού αιτήματος θα δημιουργείται αυτόματα σχετική υπόθεση ελέγχου αιτήματος προ-έγκρισης, μέσω της οποία οι αρμόδιοι χειριστές του Ειδικού Ληξιαρχείου θα μπορούν να ελέγχουν και να διαχειρίζονται τα αιτήματα.
- Θα υπάρχει διακριτό interface για δικηγόρους και πολίτες. Συγκεκριμένα οι πολίτες θα πρέπει μέσω μίας σελίδας να παρακολουθούν όλα τα αιτήματα που τους αφορούν. Αντίστοιχα οι πληρεξούσιοι δικηγόροι πρέπει να παρακολουθούν την πορεία αιτημάτων περισσοτέρων του ενός πολιτών. Συνεπώς το περιβάλλον στο οποίο θα έχουν πρόσβαση θα πρέπει να έχει μία επιπλέον οθόνη στην οποία θα εμφανίζεται η λίστα των πολιτών για λογαριασμό των οποίων έχει κατατεθεί αίτηση και μέσα από αυτή πατόντας στο όνομα του πολίτη θα γίνεται μεταφορά σε άλλη οθόνη όπου θα μπορούν να παρακολουθήσουν τα εν εξελίξει αιτήματα του συγκεκριμένου πολίτη.

- Διαδικασία Ελέγχου και Έγκρισης
  - Ανάθεση αιτήματος σε αρμόδιο χειριστή του Ειδικού Ληξιαρχείου για εξέταση της υποβληθείσας αίτησης και των εγγράφων που την συνοδεύουν.
  - Πρόσβαση του χειριστή σε όλα τα ψηφιακά έγγραφα και στοιχεία της υπόθεσης, με δυνατότητα έγκρισης ή απόρριψης των σχετικών δικαιολογητικών.
  - Αποστολή ειδοποιήσεων στους πολίτες ή στους πληρεξούσιους δικηγόρους για την ανάγκη υποβολής πρόσθετων στοιχείων και εγγράφων ή για την προ-έγκριση της αίτησης.
  - Δυνατότητα πρόσθετης υποβολής εγγράφων από τον ενδιαφερόμενο, έως ότου ολοκληρωθεί η προ-έγκριση.
  - Διασύνδεση μέσω web services με το Ολοκληρωμένο Πληροφοριακό Σύστημα Μητρώου Πολιτών (ΟΠΣ Μητρώου Πολιτών) ώστε να παρέχεται η δυνατότητα στον αρμόδιο χειριστή του Ειδικού Ληξιαρχείου να αντλεί αυτόματα και πληροφορίες που αφορούν τον αιτούντα.

- Ειδοποιήσεις και Ενημέρωση Χρηστών
  - Αυτοματοποιημένες ειδοποιήσεις μέσω email και μηνυμάτων κινητού (sms), ενημερώνοντας τους ενδιαφερόμενους για:
    i. Την παραλαβή της αίτησης από τον αρμόδιο χειριστή του Ειδικού Ληξιαρχείου.
    ii. Την πρόοδο της διαδικασίας ελέγχου,
    iii. Την ανάγκη για επιπλέον στοιχείων.
    iv. Την ολοκλήρωση της προ-έγκρισης και την ανάγκη φυσικής παρουσίας για την κατάθεση των πρωτότυπων εγγράφων.
  - Αποστολή συνδέσμου (URL) για την πρόσβαση στην ψηφιακή θυρίδα αιτημάτων και εγγράφων για πλήρη ενημέρωση των χρηστών και δυνατότητα παρακολούθηση των αιτημάτων τους.
- Εξασφάλιση Ασφάλειας και Προστασίας Προσωπικών Δεδομένων
  i. Εφαρμογή πολιτικών ασφαλείας για τη διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων.
  ii. Υψηλό επίπεδο προστασίας πρόσβασης, με καθορισμό δικαιωμάτων χρηστών βάσει ρόλων και αρμοδιοτήτων.
  iii. Αναλυτικό ιστορικό ενεργειών (audit trail / logs) για την πλήρη ιχνηλασιμότητα και την παρακολούθηση οποιασδήποτε τροποποίησης ή αλληλεπίδρασης με το σύστημα.
- Αναφορές και Στατιστικά Στοιχεία
  i. Δημιουργία αναφορών σχετικά με τον αριθμό και τον τύπο των αιτημάτων και τον χρόνο διεκπεραίωσης.
  ii. Παροχή στατιστικών δεδομένων για την αξιολόγηση της αποτελεσματικότητας της

υπηρεσίας, διευκολύνοντας τη λήψη αποφάσεων και τη βελτίωση των διαδικασιών.

Οριζόντια θα υποστηρίζεται Διαχείριση Εγγράφων, Υποθέσεων και Ροών Εργασίας, ώστε όλα τα έντυπα που υποβάλλονται από τους πολίτες και τους πληρεξούσιους δικηγόρους τους, καθώς και οι απαντήσεις από το προσωπικό του φορέα, θα αποθηκεύονται ψηφιακά με τα αντίστοιχα δικαιώματα πρόσβασης. Αυτό σημαίνει ότι κάθε έγγραφο, αίτηση ή δικαιολογητικό που κατατίθεται ψηφιακά θα καταχωρείται σε ασφαλή ηλεκτρονική πλατφόρμα. Η πρόσβαση σε αυτά τα έγγραφα θα είναι περιορισμένη στους εξουσιοδοτημένους χρήστες, διασφαλίζοντας την ιδιωτικότητα και την ασφάλεια των προσωπικών δεδομένων. Η δυνατότητα αναζήτησης και προβολής αυτών των εγγράφων θα είναι διαθέσιμη ανά πάσα στιγμή, επιτρέποντας την αποτελεσματική και άμεση διαχείριση των πληροφοριών.

Μέσω του συστήματος, οι διαδικασίες θα αυτοματοποιηθούν εξασφαλίζοντας τη βέλτιστη ροή εργασίας και την ελαχιστοποίηση των λαθών. Η διαδικασία της υποβολής αιτημάτων και του προκαταρκτικού ελέγχου θα πραγματοποιούνται ψηφιακά και αυτόματα. Το σύστημα θα παρακολουθεί και θα διαχειρίζεται κάθε στάδιο της διαδικασίας, επιτρέποντας τη συνεχή ενημέρωση των πολιτών και των πληρεξούσιων δικηγόρων τους, ενισχύοντας τελικά τη διαφάνεια, αποδοτικότητα και αξιοπιστία του φορέα.

Το σύστημα θα επιτρέπει την παρακολούθηση της κατάστασης των αιτήσεων σε πραγματικό χρόνο, από την υποβολή μέχρι την προ-έγκριση, διασφαλίζοντας διαφάνεια και σαφήνεια σε κάθε βήμα. Το σύστημα θα δίνει την δυνατότητα στους χειριστές του ληξιαρχείου να εξάγουν αναφορές και στατιστικά δεδομένα με βάση στοιχεία.

Με την ενσωμάτωση ειδοποιήσεων και αυτόματων μηνυμάτων, το σύστημα θα ενημερώνει τους πολίτες και τους πληρεξούσιους δικηγόρους τους για σημαντικές αλλαγές, διασφαλίζοντας ότι όλοι είναι ενήμεροι για τις διαδικασίες που τους αφορούν. Κάθε ενέργεια εντός του συστήματος θα καταγράφεται με τρόπο που να διασφαλίζει την ιχνηλασιμότητα και την ασφάλεια των δεδομένων, προστατεύοντας τα προσωπικά δεδομένα και διασφαλίζοντας την ακεραιότητα των πληροφοριών.

2.4 Αρχιτεκτονική Συστήματος Ψηφιακής Προ-έγκρισης Αιτημάτων Ληξιαρχικών Μητρώων

Η αρχιτεκτονική που καλείται να αναπτύξει ο Ανάδοχος, είναι πολυεπίπεδη (multi-tier), σύμφωνα με την οποία, τα δεδομένα και το περιεχόμενο αποθηκεύονται σε Βάση Δεδομένων (Database Server). Οι συναλλασσόμενοι θα έχουν πρόσβαση στο πληροφοριακό σύστημα μέσα από web browser, από εξειδικευμένες διαδικτυακές εφαρμογές φορητών συσκευών, ή/και από εξειδεικευμένες desktop εφαρμογές. Το πληροφοριακό σύστημα θα πρέπει να λειτουργεί με όλους τους διαδεδομένους web browsers (Edge, Firefox, Chrome, Opera κ.λπ.) ή/και με το λειτουργικό φορητών συσκευών. Επίσης η φυσική αρχιτεκτονική του ΟΠΣ θα πρέπει να υποστηρίζει υψηλά στάνταρ ασφάλειας για προστασία από ενδογενείς ή εξωγενείς κυβερνοαπειλές (καταγραφικό σύστημα, συστήματα κρυπτογράφησης, κα.)

Τα χαρακτηριστικά φυσικής αρχιτεκτονικής που θα πρέπει να διέπουν το σύνολο του έργου σε λειτουργικό και τεχνολογικό επίπεδο και δεδομένης της εγκατάστασης του συστήματος στο G-Cloud, είναι τα ακόλουθα:

- Σύστημα «ανοικτής» αρχιτεκτονικής (open architecture) και χρήση προτύπων που θα διασφαλίζουν:
  - Ομαλή συνεργασία και λειτουργία μεταξύ του πληροφοριακού συστήματος και των επιμέρους υποσυστημάτων του έργου.
  - Τη δικτυακή συνεργασία μεταξύ συστημάτων τα οποία βρίσκονται σε διαφορετικά υπολογιστικά

συστήματα.
  - Την επεκτασιμότητα των συστημάτων και υποσυστημάτων χωρίς αλλαγές στη δομή και αρχιτεκτονική τους.
  - Διαθεσιμότητα: αδιάλειπτη (24 ώρες Χ 7 ημέρες την εβδομάδα) παροχή υπηρεσιών στους χρήστες.
  - Ασφάλεια: προστασία από κινδύνους, ιούς, παραβίαση πρόσβασης, δημοσίευση εσφαλμένων δεδομένων.
  - Αξιοπιστία: ακρίβεια και συνέπεια παρεχόμενων υπηρεσιών.
  - Ευκολία διαχείρισης: παρακολούθηση των διαδικασιών για διασφάλιση ποιοτικής παροχής υπηρεσιών.
- Το πληροφοριακό σύστημα θα πρέπει να είναι κατάλληλα σχεδιασμένο, ώστε να παρέχει τη δυνατότητα εύκολης επικοινωνίας, διασύνδεσης, ή και ολοκλήρωσης με τρίτες εφαρμογές, ή και υποσυστήματα. Γι' αυτό το λόγο θα πρέπει να ληφθούν υπ' όψη κατ' ελάχιστον τα πρότυπα που διέπουν τη συλλογή, επεξεργασία και αποθήκευση προσωπικών δεδομένων, καθώς και οι διεθνώς αναγνωρισμένοι κανόνες και οδηγίες προσβασιμότητας από άτομα με ειδικές ανάγκες (όπως ενδεικτικά WAI (Web Accessibility Initiative- W3C), ISO-9241, ISO- 13407 κ.λπ. και βελτιωμένες εκδόσεις αυτών (http://www.w3.org/WAI/)). Σε κάθε περίπτωση πρέπει να υπάρχει απόλυτη συμμόρφωση με τον κανονισμό GDPR.
- Η φυσική αρχιτεκτονική του συστήματος θα πρέπει να εξασφαλίζει τη δικτυακή συνεργασία μεταξύ εφαρμογών, οι οποίες βρίσκονται σε εξωτερικά συστήματα, και να παρέχει τη δυνατότητα ασφαλούς διασύνδεσης και επικοινωνίας με τρίτες εφαρμογές και συσκευές βάσει διεθνών προτύπων (HTTP, WSDL, XML, JSON, REST, SOAP, OGC Web Services, UDDI, κ.λπ.).
- Αρθρωτή (modular) αρχιτεκτονική του συστήματος, ώστε να επιτρέπονται μελλοντικές επεκτάσεις και αντικαταστάσεις, ενσωματώσεις, αναβαθμίσεις ή αλλαγές διακριτών τμημάτων λογισμικού ή εξοπλισμού.
- Αρχιτεκτονική n-tier για την ευελιξία της κατανομής του κόστους και φορτίου μεταξύ κεντρικών συστημάτων και σταθμών εργασίας, για την αποδοτική εκμετάλλευση του δικτύου και την ευκολία στην επεκτασιμότητα αλλά και στη συντήρηση του.
- Χρήση συστημάτων διαχείρισης σχεσιακών βάσεων δεδομένων (RDBMS) για την ευκολία διαχείρισης μεγάλου όγκου δεδομένων, για την αυξημένη διαθεσιμότητα του συστήματος και για τη δυνατότητα ελέγχου των προσβάσεων στα δεδομένα. Θα πρέπει να διασφαλίζονται:
  - Ανοικτά τεκμηριωμένα και δημοσιευμένα συστήματα διεπαφής με προγράμματα τρίτων.
  - Ανοικτά πρωτόκολλα επικοινωνίας.
  - Ανοικτό περιβάλλον ως προς τη μεταφορά και ανταλλαγή δεδομένων με άλλα συστήματα.
- Υποστήριξη σε όλα τα επίπεδα ανοικτών, διεθνώς καθιερωμένων και ευρέως υιοθετημένων τεχνολογιών.
- Τα δομικά στοιχεία της λύσης θα πρέπει να έχουν υψηλή διαθεσιμότητα και να μην αποτελούν single point of failure.
- Οι τροποποιήσεις, βελτιώσεις και επεκτάσεις του πληροφοριακού συστήματος και των υποσυστημάτων θα πρέπει να υλοποιούνται εύκολα, γρήγορα και με το μικρότερο δυνατό κόστος.
- Θα πρέπει να υιοθετηθούν σύγχρονες και ισχυρές τεχνολογίες ασφάλειας σε επίπεδο:
  - Ισχυρών μηχανισμών πιστοποίησης της ταυτότητας των χρηστών σε όλα τα επίπεδα της αρχιτεκτονικής μέσω ειδικών authentication services, όπως SSL authentication, PKI certificates κ.λπ. Ιδιαίτερα για τους διαχειριστές του συστήματος, θα πρέπει να παρέχεται η δυνατότητα πολύ-επίπεδου (multi-factor) ελέγχου αυθεντικότητας.
  - Ισχυρών μηχανισμών auditing για ιχνηλάτηση ενεργειών χρηστών σε κάθε επίπεδο των παρεχόμενων υπηρεσιών αλλά και σε συγκεκριμένα αντικείμενα ή εγγραφές της βάσης δεδομένων.
  - Χρήσης single-sign-on μέσω διασύνδεσης με Active Directory, κλπ.
  - Σε κάθε περίπτωση, θα τηρούνται κατ ελάχιστον οι προδιαγραφές ασφαλείας των συστημάτων δικτύου και πληροφοριών όπως αναφέρονται στο Παράρτημα 1 του παρόντος εγγράφου (εφ΄όσον δεν

καλύπτονται από τα μέτρα ασφαλείας της φιλοξενούσας υποδομής G-CLOUD).

- Ενσωμάτωση στις εφαρμογές υποστήριξης άμεσης βοήθειας (on line help) και οδηγιών προς τους χρήστες ανά διαδικασία ή και οθόνη. Μηνύματα λαθών (error messages) στην Ελληνική γλώσσα και ειδοποίηση των χρηστών με όρους οικείους προς αυτούς.
- Υψηλός βαθμός παραμετροποίησης του συστήματος.
- Ικανοποίηση των παρακάτω απαιτήσεων:
  - Έλεγχος πληρότητας των στοιχείων.
  - Ακεραιότητα και ασφάλεια των δεδομένων.
- Οι ηλεκτρονικές υπηρεσίες θα πρέπει να είναι θεσμικά κατοχυρωμένες και να συμμορφώνονται πλήρως με την ισχύουσα σχετική νομοθεσία. Από το θεσμικό πλαίσιο θα καθοριστούν τα υποχρεωτικά στοιχεία και οι υποχρεωτικές λειτουργίες που πρέπει να διενεργούνται από το πληροφοριακό σύστημα.
- Υλοποίηση πολυγλωσσικών μενού για την καλύτερη εξυπηρέτηση των κατοίκων του εξωτερικού.

Λογική Αρχιτεκτονική

Το μοντέλο ανάπτυξης και λειτουργίας που θα εφαρμοστεί θα είναι πλατφόρμα Web n-tier. Θα πρέπει να στηρίζεται σε αρχιτεκτονική κατ' ελάχιστον 3 επιπέδων (3-tier architecture), η οποία περιλαμβάνει:

- Το **επίπεδο χρηστών** (client tier / presentation tier / User Interaction), που είναι υπεύθυνο για τη διεπαφή με τον τελικό χρήστη και την παρουσίαση των δεδομένων. Η πρόσβαση των χρηστών στις διαθέσιμες υπηρεσίες θα είναι μέσω μιας ενιαίας, τεχνολογικά, πλατφόρμας, όπου θα παρέχονται στον χρήστη δυνατότητες ταυτοποίησης - προσωποποίησης και εξουσιοδοτημένης πρόσβασης. Το συγκριμένο επίπεδο θα πρέπει να υλοποιηθεί με ενιαία ώριμη τεχνολογικά πλατφόρμα ώστε να είναι εύκολη η επέκτασή της με νέα λειτουργικότητα.
- Το **επίπεδο εφαρμογών** (application tier) - επιχειρησιακής λογικής (application / business logic tier), που ενσωματώνει την επιχειρησιακή λογική (business logic), δηλαδή όλους τους επιχειρησιακούς κανόνες (business rules) που διέπουν τη λειτουργία του κάθε πληροφοριακού συστήματος. Αφορά τα υποσυστήματα που καλύπτουν τη ζητούμενη λειτουργικότητα (διαδικασίες και υπηρεσίες) και τα οποία θα πρέπει να λειτουργούν σε ομοιόμορφες τεχνολογικά πλατφόρμες. Στο επίπεδο αυτό είναι απαραίτητο τα επιμέρους υποσυστήματα να είναι SOA-enabled, δηλαδή να είναι loosely-coupled και να παρέχουν τη δυνατότητα συμμετοχής σε οριζόντιες διαδικασίες ενορχήστρωσης με χρήση τεχνολογιών web services. Θα πρέπει επίσης να γίνεται διασταύρωση των στοιχείων όλων των καταχωρουμένων στο Ο.Π.Σ., ώστε να εμφανίζονται τυχούσες πολλαπλές ιδιότητες τους, για τις οποίες ενέχεται να υπάρχει ασυμβίβαστο ή σύγκρουση συμφερόντων.
- Το **επίπεδο δεδομένων** (data tier), που είναι υπεύθυνο για την αποθήκευση δεδομένων. Αφορά τα συστήματα αποθήκευσης και διαχείρισης πληροφορίας είτε αυτή αφορά transactional data (συναλλαγές), master data (πελάτης), ή δεδομένα ανάλυσης (aggregate data). Θα πρέπει τα υποσυστήματα του επίπεδου εφαρμογών να μπορούν να διαμοιράζονται τα κοινά μοντέλα δεδομένων και την κοινή υποδομή δεδομένων.

Όλα τα ανωτέρω επίπεδα χτίζονται πάνω στο Επίπεδο υποδομών (Shared Infrastructure) το οποίο αφορά τη φυσική υποδομή του συστήματος, δηλαδή τα συστήματα υλικού και την αντίστοιχη φυσική αρχιτεκτονική αυτών όπως αυτή περιγράφεται σε επόμενη παράγραφο της παρούσας.

Το πλαίσιο της λογικής αρχιτεκτονικής, ολοκληρώνουν τα κατακόρυφα επίπεδα:

- **Επίπεδο ασφαλείας** (Enterprise Security): Αφορά την υποδομή ασφαλείας που θωρακίζει το Σύστημα η οποία πρέπει να είναι ενιαία για όλη την αρχιτεκτονική και να αντιμετωπίζει με συνολικό τρόπο τα θέματα

ασφαλούς πρόσβασης χρηστών, αυτοματοποιημένης απόδοσης/ αναίρεσης δικαιωμάτων σε χρήστες, κρυπτογράφησης δεδομένων, προστασίας δεδομένων από διαρροές και εκτενούς λειτουργικότητας αναφορών για θέματα που σχετίζονται με την ασφάλεια του συστήματος.

- **Επίπεδο διαχείρισης** (Enterprise Management): Αφορά την παρεχόμενη λειτουργικότητα διαχείρισης η οποία θα επιτρέπει στον διαχειριστή να επιβλέπει τη λειτουργία όλων των επιπέδων της αρχιτεκτονικής κατά το δυνατόν από ενιαίο γραφικό ή web-based περιβάλλον και να προβαίνει σε διαχειριστικές ενέργειες αλλά και εργασίες ανίχνευσης προβλημάτων μέσα από το περιβάλλον αυτό.
- **Επίπεδο ανάπτυξης** (Enterprise Development): Αφορά τα εργαλεία αλλά και πλαίσια ανάπτυξης με τα οποία θα αναπτυχθούν τα παρεχόμενα υποσυστήματα αλλά και μέσω των οποίων η λειτουργικότητα των υποσυστημάτων θα επεκτείνεται επαναχρησιμοποιώντας την παρεχόμενη υποδομή στο πλαίσιο της υφιστάμενης αρχιτεκτονικής.

2.5 Κυβερνητικό Υπολογιστικό Νέφος G-Cloud

Το Κυβερνητικό Υπολογιστικό Νέφος G-Cloud, περιλαμβάνει την πλέον σύγχρονη πρότυπη υποδομή Κέντρου Δεδομένων (χώρος Data Center) που έχει στην κυριότητά του το Δημόσιο, σχεδιασμένη σύμφωνα με διεθνή πρότυπα (Tier III κατά Uptime Institute). Ο χώρος του Data Center φιλοξενεί την υπολογιστική υποδομή (IT) του G-Cloud και έχει σχεδιαστεί έτσι ώστε να πληροί τις υψηλότερες και αυστηρότερες διεθνείς απαιτήσεις των cloud Data Center, όσο αφορά την φυσική ασφάλεια και πρόσβαση, την ηλεκτρική παροχή, την ψύξη και τον κλιματισμό, καθώς επίσης και την πυροπροστασία και πυρόσβεση. Σε επίπεδο τηλεπικοινωνιακής υποδομής και επικοινωνίας με το διαδίκτυο, χρησιμοποιείται το Εθνικό Δίκτυο Δημόσιας Διοίκησης ΣΥΖΕΥΞΙΣ, το οποίο υποστηρίζει εδώ και 10 χρόνια με επιτυχία κομβικούς φορείς της Δημόσιας Διοίκησης. Επιπλέον, το G-Cloud περιλαμβάνει τη λειτουργία συστήματος Υπολογιστικού Κέντρου βασιζόμενο στις πλέον σύγχρονες τεχνολογίες Υπολογιστικού Νέφους και εικονικοποίησης (Cloud Computing και virtualization), το οποίο είναι δομημένο με προϊόντα τελευταίας τεχνολογίας στον χώρο του Cloud Computing και το οποίο θα παρέχει, ανάμεσα σε άλλα, τη δυνατότητα φιλοξενίας, σε υποδομές Υπολογιστικού Νέφους, Πληροφοριακών Συστημάτων Φορέων της Δημόσιας Διοίκησης. Το υπολογιστικό σύστημα του G-Cloud δομείται με προϊόντα (servers, firewalls, storage, back-up, switches, routers κ.α.) εταιρειών παγκοσμίου βεληνεκούς, απόλυτα αξιόπιστα και 100% συμβατά μεταξύ τους, δημιουργώντας ένα υπολογιστικό περιβάλλον αποδοτικό, εύκολα διαχειρίσιμο, σταθερό, διαρκώς διαθέσιμο και ασφαλές. Σημειώνεται επίσης πως το Κυβερνητικό Υπολογιστικό Νέφος G-Cloud, όσον αφορά στην ασφάλεια, έχει σχεδιαστεί και λειτουργεί με βάση το πρότυπο ISO 27001:2013, ενώ παράλληλα υποστηρίζει όλες τις διαδικασίες και τα μέτρα ασφαλείας που προβλέπονται στο κανονισμό της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΦΕΚ 799/Β/2010).

Περισσότερες πληροφορίες για το Κυβερνητικό Υπολογιστικό Νέφος (G-Cloud) μπορούν να αναζητηθούν στην ιστοσελίδα https://www.gsis.gr/dimosia-dioikisi/G-Cloud

2.6 Πίνακας Προδιαγραφών Ολοκληρωμένου Συστήματος Ψηφιακής Προ-έγκρισης Αιτημάτων Ληξιαρχικών Μητρώων

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΥΠΟΧΡ/ΚΗ ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ ΤΕΚΜΗΡΙΩΣΗΣ
1.	Εγκατάσταση του συστήματος ψηφιακής προ-έγκρισης αιτημάτων ληξιαρχικών μητρώων στο G-Cloud.	ΝΑΙ		
2.	Παροχή συστήματος για την δυνατότητα υποβολής και διαχείρισης αιτημάτων πολιτών και πληρεξούσιων δικηγόρων μέσω portal.	ΝΑΙ		
3.	Σύνδεση μέσω portal φορέα. Σε συγκεκριμένη σελίδα του portal θα πρέπει να υπάρχει εμφανές url σύνδεσης στο Σύστημα Διαχείρισης Ψηφιακής Προ-έγκρισης Αιτημάτων Ληξιαρχικών Μητρώων.	ΝΑΙ		
4.	Δυνατότητα σύνδεσης: Για τους ενδιαφερόμενους πολίτες, μέσω του Taxisnet ή θα παρέχεται εναλλακτική μέθοδος ταυτοποίησης μέσω email και κινητού τηλεφώνου, με την αποστολή κωδικού OTP (One- Time Password). Για τους πληρεξούσιους δικηγόρους, μέσω του μητρώου δικηγόρων (https://www.olomeleia.gr/)	ΝΑΙ		
5.	Περιβάλλον εργασίας όπου ο πολίτης: να μπορεί να δημιουργήσει νέα αίτηση, να έχει άμεση πρόσβαση σε όλες τις αιτήσεις που έχει κάνει, να βλέπει τις απαντήσεις σε αυτές και τα σχετικά αρχεία.	ΝΑΙ		
	ΔΗΜΙΟΥΡΓΙΑ ΝΕΑΣ ΑΙΤΗΣΗΣ			
6.	Το σύστημα θα πρέπει να διαθέτει έτοιμα templates αιτήσεων, όπου ο πολίτης να επιλέγει κάθε φορά την επιθυμητή προς συμπλήρωση και υποβολή.	ΝΑΙ		

7.	Ο πολίτης θα πρέπει να συμπληρώνει τα ελάχιστα δυνατά στοιχεία, καθώς το σύστημα θα έχει την δυνατότητα να αντλεί στοιχεία από το προφίλ του, τα οποία είναι καταχωρημένα στο TaxisNet (όπως: όνομα, ΑΦΜ, ΔΟΥ). Τα στοιχεία αυτά θα πρέπει κατά περίπτωση να μπορούν να αλλάζουν.	ΝΑΙ		
8.	Το σύστημα θα πρέπει να επιτρέπει την επισύναψη αρχείων (.docx, .pdf. .xls, .jpeg, .png κ.α.) τα οποία να συνυποβάλλονται μαζί με την αίτηση στο φορέα.	ΝΑΙ		
9.	Αφού συμπληρώσει τα στοιχεία, ο πολίτης θα πρέπει να μπορεί να την υποβάλλει οριστικά αλλά και να την αποθηκεύσει προσωρινά.	ΝΑΙ		
10.	Κατά τη διάρκεια συμπλήρωσης της αίτησης και οπωσδήποτε πριν την οριστική παραλαβή της, το σύστημα θα πρέπει να πραγματοποιεί λογικούς ελέγχους και με ανάλογα μηνύματα να καθοδηγεί το χρήστη στη διόρθωση τυχόν λαθών.	ΝΑΙ		
	ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΠΟΡΕΙΑΣ ΑΙΤΗΣΗΣ			
11.	Το σύστημα θα πρέπει να έχει ένα Ιστορικό Αιτήσεων όπου να προβάλλονται όλες οι αιτήσεις που έχει κάνει και να είναι εμφανές σε τί κατάσταση βρίσκεται η καθεμία.	ΝΑΙ		
12.	Το σύστημα θα πρέπει να ενημερώνει τον πολίτη, με ειδοποιήσεις όχι μόνο μέσα στην πλατφόρμα αλλά και με email σχετικά με την πορεία και την ολοκλήρωση της αίτησής του.	ΝΑΙ		

	ΟΛΟΚΛΗΡΩΣΗ ΑΙΤΗΣΗΣ / ΠΑΡΑΛΑΒΗ ΕΓΓΡΑΦΩΝ			
13.	Το σύστημα θα πρέπει να παρέχει μια ηλεκτρονική θυρίδα εξερχομένων εγγράφων όπου να εμφανίζονται οι απαντήσεις του φορέα μαζί με τα σχετικά έγγραφα.	ΝΑΙ		
14.	Τα σχετικά έγγραφα θα πρέπει ο πολίτης να μπορεί εύκολα να τα κατεβάσει στον υπολογιστή του ή και να τα εκτυπώσει.	ΝΑΙ		

	ΔΙΑΧΕΙΡΙΣΗ ΑΙΤΗΣΕΩΝ ΑΠΟ ΦΟΡΕΑ			
15.	Όλα τα αρχεία που υποβάλει ο πολίτης, όπως και το ίδιο το έντυπο της αίτησης, θα πρέπει να αρχειοθετούνται στην κατάλληλη υπόθεση (case), που τον αφορά.	ΝΑΙ		
16.	Με την υποβολή μιας αίτησης, αυτή θα δρομολογείται στον αρμόδιο χρήστη του σχετικού τμήματος του φορέα, το οποίο κάθε φορά θα προκύπτει από το είδος της αίτησης.	ΝΑΙ		
17.	Ανάλογα με τα βήματα που απαιτούνται για τη διαχείριση της κάθε αίτησης, αυτή θα αποστέλλεται σε όλους τους εμπλεκόμενους χρήστες του φορέα οι οποίοι θα προβαίνουν στις ανάλογες ενέργειες (π.χ. επισύναψη εγγράφου, απάντηση κ.α.).	ΝΑΙ		
18.	Για τη σύνταξη της απάντησης, ο χρήστης θα έχει στη διάθεσή του templates εγγράφων, τα οποία θα συμπληρώνει ανάλογα.	ΝΑΙ		
19.	Όταν η διαχείριση της αίτησης ολοκληρωθεί, τότε αυτή αυτόματα θα επισημαίνεται ως ολοκληρωμένη και θα μεταφέρεται στο σχετικό φάκελο των χρηστών του φορέα.	ΝΑΙ		
20.	Το σύστημα θα πρέπει να συλλέγει στοιχεία σχετικά με το χρόνο διεκπεραίωσης (ολοκλήρωσης) των αιτημάτων και να παρέχει στατιστικά στοιχεία στους αρμόδιους χρήστες, με τη μορφή λιστών, γραφημάτων και δεικτών απόδοσης (KPIs)	ΝΑΙ		
21.	Διασύνδεση μέσω web services με το Ολοκληρωμένο Πληροφοριακό Σύστημα Μητρώου Πολιτών (ΟΠΣ Μητρώου Πολιτών) ώστε να παρέχεται η δυνατότητα στον αρμόδιο χειριστή του Ειδικού Ληξιαρχείου να αντλεί αυτόματα στοιχεία και πληροφορίες που αφορούν τον αιτούντα.	ΝΑΙ		

2.7 Υπηρεσίες

2.7.1 Μελέτη Εφαρμογής – Ανάλυση Απαιτήσεων

Σκοπός της μελέτης εφαρμογής – ανάλυσης απαιτήσεων είναι η οριστικοποίηση των απαιτήσεων και των προδιαγραφών του πληροφοριακού συστήματος, η ανάλυση τεχνικών απαιτήσεων του συστήματος και ο Σχεδιασμός Αρχιτεκτονικής Λύσης.

Επιπλέον, η μελέτη εφαρμογής -ανάλυσης απαιτήσεων θα πρέπει να περιλαμβάνει την οριστικοποίηση των παρεχόμενων υπηρεσιών, την κατάρτιση του πλάνου και των σεναρίων δοκιμών αποδοχής του συστήματος, την κατάρτιση του πλάνου εκπαίδευσης των χρηστών και διαχειριστών, ώστε να εξυπηρετηθούν οι λειτουργίες του συστήματος.

2.7.2 Υπηρεσίες Ανάπτυξης και Παραμετροποίησης

Ο Ανάδοχος είναι υπεύθυνος για την ανάπτυξη, παραμετροποίηση και υλοποίηση του Συστήματος Ψηφιακής Προ-έγκρισης Αιτημάτων Ληξιαρχικών Μητρώων, ώστε να υποστηρίζει τις ανάγκες του φορέα, όπως αυτές θα οριστικοποιηθούν κατά τη φάση της Μελέτης Εφαρμογής, σύμφωνα με τις προδιαγραφές, προσαρμογή των λειτουργικών μονάδων στις απαιτήσεις του οργανισμού και ενσωμάτωση των απαιτούμενων μηχανισμών ασφαλείας και διαχείρισης δεδομένων.

2.7.3 Υπηρεσίες Εκπαίδευσης

Ο Ανάδοχος οφείλει να προσφέρει υπηρεσίες εκπαίδευσης – μεταφοράς τεχνογνωσίας στα στελέχη, χρήστες και διαχειριστές του Έργου με στόχο την πλήρη αξιοποίησή του από όλους όσους θα το χρησιμοποιούν.

Οι υπηρεσίες εκπαίδευσης θα περιλαμβάνουν κατ’ ελάχιστο τα εξής:

- Δημιουργία εκπαιδευτικού και εποπτικού υλικού εκπαίδευσης (σε ηλεκτρονική μορφή) για όλες τις κατηγορίες χρηστών που θα αναφερθούν στη συνέχεια, με βάση τις ανάγκες και τον προσδοκώμενο ρόλο στην επιχειρησιακή αξιοποίηση του Συστήματος.
- Διενέργεια εκπαίδευσης των χρηστών με βάση τον ρόλο τους.

Κάλυψη όλων των αναγκών εκπαίδευσης χρηστών που θα παρουσιαστούν κατά τη διάρκεια της πιλοτικής λειτουργίας και της περιόδου εγγύησης προκειμένου να ενταχθεί ομαλά το ΟΠΣ στην εργασιακή καθημερινότητα των χρηστών του Υπουργείου (ενδεχομένως να χρειαστεί ο ανάδοχος να επιβλέπει την hands on λειτουργία του ΟΠΣ όταν αυτό είναι αναγκαίο)

2.7.4 Υπηρεσίες Πιλοτικής Λειτουργίας

Η περίοδος πιλοτικής λειτουργίας του πληροφοριακού συστήματος αναφέρεται στο πρώτο στάδιο της πραγματικής λειτουργίας του συστήματος και περιλαμβάνει τη χρήση του συστήματος από μια περιορισμένη αλλά αντιπροσωπευτική ομάδα χρηστών, η οποία αξιοποιεί το σύνολο των λειτουργιών

του συστήματος.

Κατά την περίοδο αυτή, ο Ανάδοχος θα βρίσκεται σε συνεχή συνεργασία με τον Φορέα Λειτουργίας και θα παρέχει υποστήριξη, διαθέτοντας προσωπικό με τις κατάλληλες τεχνικές και επιχειρησιακές γνώσεις, για την υποστήριξη της πιλοτικής λειτουργίας και την εξασφάλιση της εύρυθμης λειτουργίας του συστήματος.

Βασικά κριτήρια της επιτυχούς ολοκλήρωσης της περιόδου πιλοτικής λειτουργίας του συστήματος είναι να εντοπιστούν και να απαλειφθούν όλα τα λάθη του λογισμικού εφαρμογών (debugging) και να εντοπιστούν και να απαλειφθούν τα κρίσιμα λειτουργικά λάθη (critical functional errors) του συστήματος που επηρεάζουν άμεσα την επιχειρησιακή λειτουργία του ΑΠΘ.

2.7.5 Υπηρεσίες Εγγύησης - Συντήρησης – Υποστήριξης & Helpdesk

Οι Υπηρεσίες συντήρησης και υποστήριξης περιλαμβάνουν, ενδεικτικά, την υποστήριξη και αποκατάσταση βλαβών, τη διασφάλιση καλής λειτουργίας του συνολικού συστήματος, τον εντοπισμό αιτιών βλαβών / δυσλειτουργιών και την αποκατάστασή τους. Κατόπιν ειδοποίησης από τον Φορέα Λειτουργίας του Έργου, ο Ανάδοχος είναι υποχρεωμένος να επιλύει τα προβλήματα εντός συγκεκριμένου χρονικού διαστήματος. Η επίλυση των προβλημάτων γίνεται υπό συνθήκες εγγυημένου επιπέδου υπηρεσιών. Στις παραπάνω υπηρεσίες περιλαμβάνεται η λειτουργία Helpdesk.

Βασική υποχρέωση του Αναδόχου είναι η οργάνωση και λειτουργία σύγχρονου Γραφείου Υποστήριξης (HelpDesk) το οποίο θα είναι διαθέσιμο προς όλους τους χρήστες του συστήματος (χρήστες Υπουργείου Εσωτερικών, πολίτες, δικηγόρους κ.λ.π) σε ώρες ΚΩΚ (09.00-17.00).

Οι υπηρεσίες Helpdesk θα πρέπει να προσφερθούν από τον Ανάδοχο κατά τη Φάση Δοκιμαστικής Λειτουργίας του Έργου, κατά την περίοδο εγγύησης και, εφόσον υπογραφεί σχετική σύμβαση, κατά την περίοδο συντήρησης.

Στο πλαίσιο της υπηρεσίας αυτής ο Ανάδοχος αναλαμβάνει τα ακόλουθα:

- Να καταγράφει τα χαρακτηριστικά στοιχεία των βλαβών που αναφέρονται από το προσωπικό της Υπηρεσίας. Κάθε περιστατικό πρέπει να λαμβάνει ένα μοναδικό κλειδί αναφοράς και να καταγράφεται τουλάχιστον η εξής πληροφορία: Υπηρεσία, είδος (υποσύστημα), περιγραφή βλάβης, ώρα αναγγελίας. Η αναγγελία βλαβών θα μπορεί να γίνει, εναλλακτικά, με όλους τους παρακάτω τρόπους:
  - Τηλέφωνο
  - Email
  - ειδική web εφαρμογή που πρέπει να διαθέτει ο Ανάδοχος, από την οποία καταγράφονται, κατ’ ελάχιστο, ο χρόνος έναρξης και λήξης του προβλήματος, η περιγραφή του και οι ενέργειες επίλυσης, καθώς και ο υπεύθυνος για κάθε ενέργεια.
- Ο Ανάδοχος θα πρέπει να συνεργαστεί με τον Φορέα Λειτουργίας για την ενημέρωση και ορθή λειτουργία της εφαρμογής καταγραφής προβλημάτων με τα απαραίτητα στοιχεία που αφορούν στο συγκεκριμένο Έργο.
- Ο Ανάδοχος θα πρέπει να παρέχει **ένα (1) έτος** εγγύηση του συστήματος.

2.8 Προδιαγραφές Ασφαλείας των Συστημάτων Δικτύου και Πληροφοριών

2.8.1 Καταγραφή Υλικού και Λογισμικού

Ο ανάδοχος θα πρέπει να παραδώσει επικαιροποιημένο μητρώο υλικού, λογισμικού και πληροφορίας για το Πληροφοριακό Σύστημα και σχηματική αποτύπωση της υποδομής

2.8.2 Ασφαλής Παραμετροποίηση Εξοπλισμού και Εφαρμογών

Ο ανάδοχος θα πρέπει

i. να παραδώσει πολιτική και διαδικασίες ασφαλούς παραμετροποίησης εξοπλισμού, λειτουργικών συστημάτων και εφαρμογών

ii. να εφαρμόζει εγκεκριμένη διαδικασία ασφαλούς παραμετροποίησης (secure configuration process), με βάση διεθνώς αποδεκτά πρότυπα και οδηγίες των κατασκευαστών των servers και των δικτυακών συσκευών, τα οποία και θα αναφέρει.

iii. να χρησιμοποιεί μόνο υποστηριζόμενες εκδόσεις για τα λειτουργικά συστήματα των σταθμών εργασίας, των servers και των δικτυακών συσκευών.

iv. να κάνει λήψη των ενημερώσεων ασφάλειας και των αναβαθμίσεων λογισμικού για τα λειτουργικά συστήματα των σταθμών εργασίας, των servers και των δικτυακών συσκευών με αυτοματοποιημένο τρόπο, κατ' ελάχιστο σε μηνιαία βάση.

v. να χρησιμοποιεί μόνο τις τελευταίες και ενημερωμένες εκδόσεις για κάθε server εφαρμογή του που είναι προσβάσιμη από το Internet.

vi. να υλοποιεί τις παρακάτω ρυθμίσεις στις δικτυακές συσκευές:

- Απενεργοποίηση κάθε περιττής υπηρεσίας (service).
- Στα switches ενεργοποίηση της λειτουργίας "port security".
- Στους δρομολογητές (routers) απενεργοποίηση των interfaces και των πρωτόκολλων δρομολόγησης που δεν χρησιμοποιούνται.
- Στα switches απενεργοποίηση των θυρών που δεν χρησιμοποιούνται.
- Εφαρμογή αυθεντικοποίησης δύο παραγόντων (2-factor authentication) για την πρόσβαση στο διαχειριστικό περιβάλλον όλων των κρίσιμων δικτυακών συσκευών.
- Διασφάλιση ότι σε όσα συστήματα έχουν ταξινομηθεί ως κρίσιμα δεν είναι εφικτή η σύνδεση φορητών μέσων αποθήκευσης (USB, εξωτερικών σκληρών δίσκων, CD, DVD), εάν δεν υπάρχει γι’ αυτό αυστηρή επιχειρησιακή ανάγκη.
- Διασφάλιση ότι τα προεπιλεγμένα συνθηματικά (default passwords) σε κάθε νέο προϊόν τροποποιούνται κατά την πρώτη εγκατάσταση του προϊόντος.
- Τήρηση πλήρων αντίγραφων ασφαλείας (system images) των λειτουργικών συστημάτων του, με τις βασικές ρυθμίσεις ασφάλειας, σε κρυπτογραφημένη μορφή, με περιορισμούς στην πρόσβαση και με έλεγχο ακεραιότητας των αρχείων (file integrity monitoring).

2.8.3 Έλεγχος Εκτέλεσης Προγραμμάτων και Υπηρεσιών

Ο ανάδοχος θα πρέπει να:

- έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στον έλεγχο εγκατάστασης και εκτέλεσης προγραμμάτων και υπηρεσιών στο δίκτυο και στα συστήματά του.
- διασφαλίζει ότι στους servers και στους σταθμούς εργασίας λειτουργούν μόνο οι θύρες (ports), τα πρωτόκολλα και οι δικτυακές υπηρεσίες που είναι απαραίτητες για τη διεκπεραίωση των επιχειρησιακών λειτουργιών του.
- διασφαλίσει ότι αν υπάρξει επιχειρησιακή ανάγκη σε χρήστες με standard δικαιώματα (non-privileged) να εγκαταστήσουν λογισμικό, αυτό μπορεί να συμβεί μόνο με εγκεκριμένες εφαρμογές που αποθηκεύονται σε αποθετήρια λογισμικού που ελέγχονται από τον Οργανισμό.
- έχει δημιουργήσει κατάλογο με εξουσιοδοτημένες εφαρμογές και συστατικά τους (βιβλιοθήκες, αρχεία διαμόρφωσης κ.α.) και να έχει διασφαλίσει ότι μόνο αυτές θα επιτρέπεται να εκτελούνται στους servers και στους σταθμούς εργασίας (application whitelisting).
- εφαρμόζει κατάλληλες τεχνικές, έτσι ώστε μόνο εγκεκριμένα scripts, δηλαδή συγκεκριμένα .ps1, py κ.λπ. αρχεία να επιτρέπεται να εκτελούνται. Η εκτέλεση μη εγκεκριμένων scripts εμποδίζεται.
- διενεργεί σε τακτική βάση αυτοματοποιημένο port scanning στο σύνολο της υποδομής του πληροφοριακού συστήματος με σκοπό την ανίχνευση μη εξουσιοδοτημένων ανοικτών δικτυακών θυρών και υπηρεσιών σε συστήματα.
- διασφαλίσει ότι οι χρήστες με standard δικαιώματα (non-privileged) δεν μπορούν να απενεργοποιήσουν ή να τροποποιήσουν τις ρυθμίσεις ασφάλειας στο λειτουργικό τους σύστημα.
- υλοποιήσει κατάλληλες ρυθμίσεις στο firewall της εξωτερικής περιμέτρου του δικτύου, ώστε αυτό να εμποδίζει την εισερχόμενη από και εξερχόμενη προς το Internet επικοινωνία στις παρακάτω θύρες: TCP 445 (SMB), UDP 137 (NetBIOS Name Resolution), UDP 138 (NetBIOS Datagram Service) και TCP 139 (NetBIOS Session Service).
- υλοποιεί κατάλληλες ρυθμίσεις ώστε να εμποδίζονται οι εισερχόμενες SMB συνδέσεις στην TCP θύρα 445 σε όσους σταθμούς εργασίας και servers δεν φιλοξενούν κοινόχρηστο περιεχόμενο (shares).
- έχει απενεργοποιήσει τις εκδόσεις SMBv1 και v2 στο εσωτερικό δίκτυο και να έχει αναβαθμίσει στην έκδοση v3 ή στην πλέον πρόσφατη.

2.8.4 Διαχείριση Λογαριασμών και Έλεγχος Πρόσβασης

Ο ανάδοχος θα πρέπει να :

i. τηρεί την καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στη διαχείριση των λογαριασμών χρηστών και στον έλεγχο πρόσβασης στο δίκτυο, στα συστήματα, στις εφαρμογές και στα δεδομένα του.

ii. έχει διασφαλίσει ότι οι χρήστες, το προσωπικό του και οι εξωτερικοί συνεργάτες που

αποκτούν λογαριασμό χρήστη αναγνωρίζονται (identified) με μοναδικό τρόπο, με σκοπό τη διασφάλιση λογοδοσίας (accountability).

iii. έχει απενεργοποιήσει τους προεπιλεγμένους (default) λογαριασμούς στα αγαθά και στο λογισμικό του, όπως είναι οι root, administrator ή και άλλοι προϋπάρχοντες εταιρικοί λογαριασμοί.

iv. τηρεί στο σύστημα κατάλογο (inventory) με όλους τους λογαριασμούς χρηστών, ο οποίος περιέχει κατ' ελάχιστον το ονοματεπώνυμο, την ημερομηνία έναρξης / λήξης, τα προνόμια και την Υπηρεσία εργασίας του υπαλλήλου.

v. τηρεί κατάλογο (inventory) με όλους τους λογαριασμούς υπηρεσιών (service accounts) που χρησιμοποιούνται. Ο κατάλογος θα πρέπει να περιέχει κατ' ελάχιστο τον ιδιοκτήτη (owner), το σκοπό και την ημερομηνία αναθεώρησης.

vi. έχει υλοποιήσει μηχανισμό για να απενεργοποιεί λογαριασμούς χρηστών ύστερα από συγκεκριμένο χρονικό διάστημα αδρανούς δραστηριότητας (π.χ. 3 μήνες).

vii. εκχωρεί δικαιώματα πρόσβασης με βάση διακριτούς ρόλους, έτσι ώστε οι χρήστες να έχουν πρόσβαση αποκλειστικά και μόνο στο είδος της πληροφορίας που είναι απαραίτητη για την εκτέλεση των εργασιακών καθηκόντων τους, με βάση τις αρχές των ελάχιστων προνομίων (least privilege) και της ανάγκης γνώσης (need to know).

viii. διασφαλίζει ότι στους χρήστες που εκτελούν αποκλειστικά μη διαχειριστικές εργασίες καθημερινής ρουτίνας (π.χ. χρήση προγραμμάτων word, excel, adobe reader, ανάγνωση και αποστολή e-mail, περιήγηση στο Internet κ.λπ.) χορηγείται αποκλειστικά standard λογαριασμός απλού χρήστη (non-privileged account).

ix. διασφαλίζει ότι στους χρήστες που λόγω καθηκόντων εκτελούν διαχειριστικές εργασίες χορηγείται λογαριασμός αυξημένων προνομίων που χρησιμοποιείται αποκλειστικά για τις εργασίες αυτές. Οι εν λόγω λογαριασμοί δεν έχουν πρόσβαση σε υπηρεσίες email και Internet.

x. διασφαλίζει ότι στους χρήστες που λόγω καθηκόντων έχουν λογαριασμό αυξημένων προνομίων (privileged account) χορηγείται δεύτερος standard λογαριασμός απλού χρήστη (non-privileged account) για την εκτέλεση μη διαχειριστικών εργασιών καθημερινής ρουτίνας (π.χ. χρήση προγραμμάτων word, excel, adobe reader, ανάγνωση και αποστολή e-mail, περιήγηση στο Internet κ.λπ.).

xi. έχει υλοποιήσει κεντρική διαχείριση λογαριασμών μέσω υπηρεσίας καταλόγου (π.χ. Active directory service).

xii. εφαρμόζει την τεχνική της «διπλής εξουσιοδότησης» ("dual authorization"), έτσι ώστε να απαιτείται η έγκριση δύο εξουσιοδοτημένων χρηστών για την εκτέλεση ιδιαίτερα κρίσιμων και ευαίσθητων εντολών ή λειτουργιών.

2.8.5 Αυθεντικοποίηση Χρηστών

Ο ανάδοχος θα πρέπει:

i. να τηρεί την καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στην αυθεντικοποίηση των χρηστών, με σκοπό την αποφυγή μη εξουσιοδοτημένης πρόσβασης στα

πληροφοριακά του συστήματα.

ii. να υλοποιεί μηχανισμούς αυθεντικοποίησης που επιβάλλουν τη δημιουργία ισχυρών κωδικών πρόσβασης για τα πληροφοριακά του συστήματα. Ως ισχυροί κωδικοί πρόσβασης θεωρούνται εκείνοι που έχουν μήκος τουλάχιστον δώδεκα (12) χαρακτήρων και περιέχουν σωρευτικά τουλάχιστον ένα (1) κεφαλαίο γράμμα, ένα (1) μικρό γράμμα, έναν (1) αριθμό και έναν (1) ειδικό χαρακτήρα και δεν περιέχουν ονόματα ή κοινές λέξεις που υπάρχουν σε λεξικά. Οι μηχανισμοί δημιουργίας ισχυρών κωδικών μπορεί να περιλαμβάνουν και τη δυνατότητα δημιουργίας φράσεων (passphrases)

iii. να εφαρμόζει πολυπαραγοντική αυθεντικοποίηση (multi-factor authentication) για όλες τις απομακρυσμένες συνδέσεις (remote access connections) στο δίκτυό του. Η εν λόγω απαίτηση υλοποιείται για το σύνολο των υπαλλήλων του φορέα (σε μη προνομιούχους και σε διαχειριστικούς λογαριασμούς), καθώς και για τρίτα μέρη στα πλαίσια συμβατικής τους υποχρέωσης για παροχή υπηρεσιών υποστήριξης ή συντήρησης των συστημάτων του Οργανισμού.

iv. να εφαρμόζει πολυπαραγοντική αυθεντικοποίηση (multi-factor authentication) για κάθε χρήστη που επιθυμεί πρόσβαση σε κρίσιμα ή ευαίσθητα δεδομένα.

v. να έχει ορίσει μέγιστο όριο (τριών έως πέντε) συνεχόμενων ανεπιτυχών προσπαθειών για είσοδο (log in) σε λογαριασμό, πέραν των οποίων ο λογαριασμός θα κλειδώνει για ένα προκαθορισμένο χρονικό διάστημα.

vi. να διασφαλίζει ότι οι κωδικοί πρόσβασης αποθηκεύονται σε κρυπτογραφημένη μορφή. Η κρυπτογράφηση γίνεται με τη χρήση one-way hash αλγορίθμων με την επιπλέον προσθήκη στον υπολογισμό μίας ακολουθίας τυχαίων δεδομένων (salt).

vii. να εφαρμόζει πολυπαραγοντική αυθεντικοποίηση (multi-factor authentication) με αποστολή one-time password με χρήση mobile εφαρμογής αντί για SMS.

2.8.6 Ασφάλεια Δικτύων

Ο ανάδοχος θα πρέπει:

i. να τηρεί επικαιροποιημένο διάγραμμα δικτύου και ροής δεδομένων (network and data flow diagram), στο οποίο απεικονίζονται όλες οι δικτυακές συνδέσεις

ii. να τηρεί σε προστατευμένο αρχείο όλους τους κανόνες δρομολόγησης, καθώς και τους κανόνες ελέγχου πρόσβασης (access control lists) των firewalls.

iii. να εξασφαλίσει ότι οι servers που έχουν δημόσια IP διεύθυνση (π.χ. web servers, mail servers, VPN servers κ.λπ.) ανήκουν σε διακριτή δικτυακή ζώνη (υποδίκτυο) που είναι διαχωρισμένη με φυσικό ή λογικό τρόπο από το εσωτερικό δίκτυο. Η υλοποίηση αυτή ονομάζεται αποστρατικοποιημένη ζώνη (de-militirized zone - DMZ).

iv. να έχει εγκαταστήσει firewall στην εξωτερική περίμετρο του δικτύου, το οποίο επιτρέπει μόνο την εισερχόμενη και εξερχόμενη ροή της πληροφορίας (inbound και outbound traffic) που είναι απαραίτητη για την εκτέλεση των επιχειρησιακών λειτουργιών του.

v. να εφαρμόζει φιλτράρισμα της δικτυακής κίνησης (traffic filtering) μεταξύ των υποδικτύων με σκοπό να περιορίσει τη ροή της πληροφορίας στην απολύτως απαραίτητη για τις επιχειρησιακές ανάγκες του.

vi. να διασφαλίζει ότι η απομακρυσμένη πρόσβαση χρηστών στο εσωτερικό δίκτυό του γίνεται μέσω VPN (Virtual Private Network), με χρήση αυθεντικοποίησης δύο παραγόντων (2-factor authentication) και των πιο πρόσφατων αλγόριθμων κρυπτογράφησης.
vii. να υλοποιεί firewall επιπέδου εφαρμογής (application firewall) μπροστά από κάθε κρίσιμης σημασίας server, με σκοπό τον αποκλεισμό της κακόβουλης κίνησης.
viii. να υλοποιήσει δικτυακά συστήματα ανίχνευσης και πρόληψης εισβολών (network intrusion detection / prevention systems), με σκοπό την ανίχνευση και πρόληψη επιθέσεων.
ix. να έχει διασφαλίσει ότι η υποδομή του διαθέτει πλεονασμό σε πόρους που της επιτρέπουν να ανθίσταται σε επίθεση άρνησης παροχής υπηρεσιών.
x. να έχει διαχωρίσει δικτυακά τις κρίσιμες υπηρεσίες του από άλλες υπηρεσίες που είναι πιθανότερο να στοχοποιηθούν (π.χ. web υπηρεσίες).
xi. να υλοποιεί συστήματα παρακολούθησης της διαθεσιμότητας των κρίσιμων υπηρεσιών του, που ανιχνεύουν επιθέσεις άρνησης παροχής υπηρεσιών και στέλνουν ειδοποίηση σε πραγματικό χρόνο.
xii. να υλοποιεί δίοδο δεδομένων (data diode) σε μορφή hardware, το οποίο επιβάλλει τη ροή δεδομένων μόνο προς μία κατεύθυνση με σκοπό την προστασία κρίσιμης πληροφορίας σε υποδίκτυα υψηλών απαιτήσεων ασφάλειας.

2.8.7 Τήρηση και ανάλυση αρχείων καταγραφής συμβάντων (event logs)

Ο ανάδοχος θα πρέπει να :

i. έχει ενεργοποιήσει τη λειτουργία καταγραφής συμβάντων (event logs) σε όλους τους σταθμούς εργασίας, servers και δικτυακές συσκευές.
ii. έχει διασφαλίσει τον συγχρονισμό ανάμεσα στα ρολόγια όλων των συσκευών, έτσι ώστε να επιτυγχάνεται ακρίβεια στη συσχέτιση συμβάντων μεταξύ διαφορετικών συστημάτων.
iii. έχει ενεργοποιήσει την καταγραφή επιτυχούς και ανεπιτυχούς εισόδου (login) και εξόδου
iv. (logout) για όλα τα συστήματα που απαιτούν αυθεντικοποίηση.
v. έχει ενεργοποιήσει την καταγραφή όλων των δραστηριοτήτων που αφορούν σε διαχειριστικούς λογαριασμούς.
vi. έχει διασφαλίσει ότι καταγράφονται τα παρακάτω συμβάντα: Πρόσβασης σε αρχεία και διεργασίες διακομιστών (servers), Αποτυχημένων προσπαθειών εκτέλεσης αρχείων, Χρήσης και απόπειρας χρήσης ειδικών προνομίων, Χρήσης των εφαρμογών συστήματος, Αλλαγών σε λογαριασμούς και στην πολιτική ασφάλειας, Αιτημάτων HTTP και DNS, Μεταφοράς δεδομένων από και προς φορητά μέσα αποθήκευσης.
vii. έχει ρυθμίσει τα αρχεία καταγραφής συμβάντων να περιλαμβάνουν λεπτομερή metadata όπως πηγή γεγονότος, ημερομηνία, χρήστης, χρονοσήμανση, IP διεύθυνση πηγής, IP διεύθυνση προορισμού κ.λπ.
viii. έχει διασφαλίσει ότι τα αρχεία καταγραφής συμβάντων τηρούνται για χρονική περίοδο κατ' ελάχιστον ενός (1) έτους.
ix. έχει διασφαλίσει ότι τα αρχεία καταγραφής συμβάντων προστατεύονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση και διαγραφή.
x. έχει διασφαλίσει ότι η διαχείριση της λειτουργίας καταγραφής συμβάντων έχει ανατεθεί σε ένα υποσύνολο χρηστών με λογαριασμούς αυξημένων προνομίων.

2.8.8 Ασφάλεια Διαδικτυακών Εφαρμογών

Ο ανάδοχος θα πρέπει:

i. να ορίζει τις απαιτήσεις ασφάλειας για κάθε εφαρμογή που πρόκειται να αναπτυχθεί, είτε in-house είτε outsourced. Οι απαιτήσεις ανταποκρίνονται στο βαθμό κρισιμότητας των λειτουργιών της εφαρμογής και της ευαισθησίας των δεδομένων που επεξεργάζεται.
ii. να διασφαλίζει ότι χρησιμοποιούνται αξιόπιστες και πλήρως ενημερωμένες πλατφόρμες ανάπτυξης εφαρμογών, καθώς και βιβλιοθήκες λογισμικού που προέρχονται από έμπιστες πηγές και συντηρούνται ενεργά.
iii. να διασφαλίζει ότι εφαρμόζονται τεχνικές ασφαλούς ανάπτυξης λογισμικού (secure development lifecycle) καθ' όλη τη διάρκεια του κύκλου ζωής των διαδικτυακών εφαρμογών του (σχεδιασμός, ανάπτυξη, δοκιμές, παραγωγική λειτουργία, συντήρηση), είτε αυτές έχουν αναπτυχθεί in-house είτε outscourced.
iv. να διασφαλίζει ότι κατά την ανάπτυξη διαδικτυακών εφαρμογών λαμβάνονται υπόψη κοινοί τύποι ευπαθειών, όπως είναι το OWASP Top-10.
v. να διασφαλίζει ότι κατά την ανάπτυξη διαδικτυακών εφαρμογών όλα τα δεδομένα εισόδου (πεδία φορμών HTML, αιτήματα REST, παράμετροι URL, κεφαλίδες (headers) HTTP, cookies, αρχεία batch, RSS feeds κ.α.) επικυρώνονται συντακτικά και σημασιολογικά (input validation) με τη χρήση white-list filtering στην πλευρά του server.
vi. να διασφαλίζει ότι κάθε επικοινωνία του web server (με browsers χρηστών, κλήσεις άλλων web υπηρεσιών, βάσεις δεδομένων, cloud κ.α.) υλοποιείται με κρυπτογράφηση της σύνδεσης με χρήση της πλέον πρόσφατης έκδοσης του πρωτοκόλλου TLS (encryption in transit).
vii. να διασφαλίζει ότι κατά την ανάπτυξη των εφαρμογών υλοποιούνται τεχνικές ελέγχου και διαχείρισης λαθών και εξαιρέσεων (errors and exceptions) για κάθε είδος εισερχόμενων δεδομένων, λαμβάνοντας υπόψη τον τύπο, το μέγεθος, τη μορφή και το αποδεκτό εύρος τιμών.
viii. να διασφαλίζει ότι οι διαδικτυακές εφαρμογές του, ανεπτυγμένες είτε in-house είτε outsourced, υλοποιούν τα παρακάτω γνωρίσματα: Επιτρέπουν μόνο ισχυρούς κωδικούς πρόσβασης, Εφαρμόζουν αυθεντικοποίηση δύο παραγόντων (2-factor authentication), όπου ορίζουν οι απαιτήσεις ασφάλειας της εφαρμογής, Υλοποιούν την αρχή των ελάχιστων προνομίων (least privilege), Υλοποιούν τεχνικές παραμετροποίησης ερωτημάτων (query parameterization) σε κάθε στοιχείο που εισάγεται στο σύστημα διαχείρισης βάσεων δεδομένων της εφαρμογής, Υλοποιούν τεχνικές κωδικοποίησης χαρακτήρων (output encoding και character escaping) ακριβώς πριν τα δεδομένα εισόδου εισέλθουν στο διερμηνευτή (interpreter) της εφαρμογής, Οι κεφαλίδες απάντησης (response headers) του πρωτοκόλλου HTTP έχουν ρυθμιστεί ώστε να υλοποιούν τα Content-Security-Policy, HSTS και X-Frame-Options, Σε κάθε αυθεντικοποίηση χρήστη η εφαρμογή δημιουργεί ένα νέο token συνόδου (session token) με τη χρήση εγκεκριμένων κρυπτογραφικών αλγορίθμων, Κατά την αποσύνδεση του χρήστη (logout) και τη λήξη της συνόδου το token συνόδου ακυρώνεται, έτσι ώστε η χρήση του back button δεν επαναφέρει μία αυθεντικοποιημένη σύνοδο, Τα

δεδομένα της εφαρμογής που έχουν ταξινομηθεί ως κρίσιμα / ευαίσθητα αποθηκεύονται σε κρυπτογραφημένη μορφή (encryption at rest), Τα tokens συνόδου που βασίζονται σε cookies έχουν ενεργοποιημένες τις ιδιότητες (attributes) “Secure”, “HttpOnly”, “SameSite” και το prefix " Host-". διασφαλίζει ότι διενεργείται έλεγχος ευπαθειών (vulnerability test) για κάθε νέα λειτουργικότητα που προστίθεται στην εφαρμογή κατά τα διαδοχικά στάδια ανάπτυξής της.

ix. να διασφαλίζει ότι διενεργείται έλεγχος παρείσδυσης (penetration test) πριν η τελική έκδοση της εφαρμογής τεθεί σε παραγωγική λειτουργία.
x. να εφαρμόζει την τεχνική TLS inspection, με την οποία η διαδικτυακή κίνηση που μεταφέρεται μέσω HTTPS συνδέσεων αποκρυπτογραφείται και επιθεωρείται με σκοπό την ανίχνευση κακόβουλου περιεχομένου.
xi. να υλοποιεί firewall επιπέδου web εφαρμογής (web application firewall), είτε στην υποδομή του είτε ως ανατιθέμενη cloud υπηρεσία (security as a service), το οποίο ελέγχει την HTTP κίνηση προς τις διαδικτυακές εφαρμογές του για γνωστούς τύπους επιθέσεων. Ο Οργανισμός έχει εγκαταστήσει σύστημα ασφάλειας πληροφοριών και διαχείρισης συμβάντων (Security Information and Event Management - SIEM), με σκοπό τη συγκέντρωση των αρχείων καταγραφής συμβάντων σε κεντρικό σημείο και την ανάλυση και συσχέτισή τους για τον εντοπισμό ύποπτης δραστηριότητα.

2.8.9 Χρήση Κρυπτογραφίας

Ο ανάδοχος θα πρέπει να:
i.διασφαλίζει ότι τα δεδομένα που έχουν ταξινομηθεί ως κρίσιμα / ευαίσθητα κρυπτογραφούνται κατά τη μετάδοσή τους (encryption in transit).
ii.διασφαλίζει ότι τα δεδομένα που έχουν ταξινομηθεί ως κρίσιμα / ευαίσθητα κρυπτογραφούνται κατά την αποθήκευσή τους (encryption at rest). Τα εν λόγω δεδομένα μπορεί να βρίσκονται σε διακομιστές, εφαρμογές και βάσεις δεδομένων.
iii.διασφαλίζει ότι κατά την κρυπτογράφηση χρησιμοποιούνται μόνο τελευταίες εκδόσεις εγκεκριμένων κρυπτογραφικών πρωτοκόλλων και λογισμικού, καθώς επίσης και το κατάλληλο μήκος κλειδιών.
iv.κατά τη χρήση της κρυπτογραφίας, να χρησιμοποιεί τους παρακάτω κρυπτογραφικούς αλγόριθμους: Για την υλοποίηση συμμετρικής κρυπτογράφησης χρησιμοποιείται ο αλγόριθμος AES, με μήκος κλειδιού 128, 192 ή 256 bits. Για την υλοποίηση ψηφιακών υπογραφών χρησιμοποιείται ο αλγόριθμος RSA με μήκος κλειδιού τουλάχιστον 2048 bits ή ο αλγόριθμος ECDSA με μήκος κλειδιού τουλάχιστον 224 bits.Για την υλοποίηση αλγορίθμων κατακερματισμού (π.χ. ψηφιακές υπογραφές κ.α.) χρησιμοποιείται ο Secure Hash Algorithm 2 (SHA-2), με επιλογή μεταξύ των SHA-256, SHA-384 ή SHA-512.
v.Να υλοποιεί συνολική διαχείριση (δημιουργία, αποθήκευση, έλεγχος, διανομή) συμμετρικών και ασύμμετρων κλειδιών κρυπτογράφησης χρησιμοποιώντας διεθνώς αποδεκτά πρότυπα και διαδικασίες, συμπεριλαμβανομένων αυστηρών κανόνων πρόσβασης στην πλατφόρμα διαχείρισης.
vi.να χρησιμοποιεί αυθεντικοποίηση δημοσίου κλειδιού (public key-based authentication) για την υλοποίηση SSH (Secure Shell) συνδέσεων.

2.8.10 Υλοποίηση Τεχνικών Κυβερνοασφάλειας

Ο ανάδοχος θα πρέπει να:

i. διενεργεί σε τακτική βάση (π.χ. μία φορά το μήνα) αυτοματοποιημένη σάρωση ευπαθειών στα πληροφοριακά του συστήματα, προκειμένου να εντοπιστούν δυνητικές ευπάθειες στο δίκτυο, στα συστήματα και στις εφαρμογές του.
ii. υλοποιεί εγκεκριμένη διαδικασία επιδιόρθωσης των ευπαθειών που έχουν ανιχνευθεί στα αγαθά του σε μηνιαία βάση.
iii. διενεργεί σε περιοδική βάση (π.χ. μία φορά ετησίως) πλήρη αξιολόγηση των ευπαθειών στα πληροφοριακά του συστήματα (vulnerability assessment).
iv. διενεργεί σε περιοδική βάση (π.χ. μία φορά ετησίως) εξωτερικό έλεγχο παρείσδυσης (external penetration test), με σκοπό την προσομοίωση κυβερνοεπίθεσης που εκκινεί έξω από τη δικτυακή περίμετρο του Οργανισμού.
v. διενεργεί σε περιοδική βάση (π.χ. μία φορά ετησίως) εσωτερικό έλεγχο παρείσδυσης (internal penetration test), με σκοπό την προσομοίωση κυβερνοεπίθεσης στο εσωτερικό δίκτυο.
vi. διενεργεί σε περιοδική βάση (π.χ. μία φορά ετησίως) ασκήσεις "κόκκινης / μπλε ομάδας" ("red team / blue team" exercises), με σκοπό την προσομοίωση κυβερνοεπιθέσεων από γνωστές υψηλού προφίλ ομάδες κυβερνοεγκληματιών.
vii. υλοποιεί εγκεκριμένη διαδικασία επιδιόρθωσης των ευρημάτων που εντοπίζονται στους ελέγχους παρείσδυσης ή στις ασκήσεις "κόκκινης / μπλε ομάδας" με βάση σαφές πλάνο προτεραιοποίησης. Επίσης, να υλοποιεί διαδικασία επικύρωσης των πρόσθετων μέτρων ασφάλειας που απαιτούνται για την επιδιόρθωση.

2.8.11 Λήψη Αντιγράφων Ασφάλειας

Ο ανάδοχος θα πρέπει να:

i. έχει διασφαλίσει ότι λαμβάνονται αντίγραφα ασφαλείας με αυτοματοποιημένο τρόπο από όλα τα σημαντικά πληροφοριακά του συστήματα σε ημερήσια βάση, συνδυάζοντας με τον κατάλληλο τρόπο τις διαθέσιμες τεχνολογίες.
ii. έχει διασφαλίσει ότι τα ληφθέντα αντίγραφα ασφαλείας προστατεύονται με κρυπτογράφηση κατά τη μεταφορά τους (encryption in transit).
iii. έχει διασφαλίσει ότι τα ληφθέντα αντίγραφα ασφαλείας προστατεύονται με επαρκή μέτρα ασφάλειας κατά την αποθήκευσή τους. Παραδείγματα αποτελούν η κρυπτογράφηση, η πολυπαραγοντική αυθεντικοποίηση, ο έλεγχος πρόσβασης κ.α.
iv. έχει διασφαλίσει ότι τα αντίγραφα ασφαλείας αποθηκεύονται σε τουλάχιστον έναν (1) offline προορισμό που δεν είναι συνδεδεμένος σε κάποιο δίκτυο.
v. διενεργεί έλεγχο ακεραιότητας των αντιγράφων ασφαλείας σε περιοδική βάση.
vi. διενεργεί δοκιμή επαναφοράς δεδομένων (restoration) σε περιοδική βάση, με σκοπό την επικύρωση ότι η λήψη αντιγράφων ασφαλείας λειτουργεί με σωστό τρόπο.
vii. αποθηκεύει τα ληφθέντα αντίγραφα ασφαλείας σε διαφορετικές γεωγραφικά διεσπαρμένες τοποθεσίες.

2.8.12 Χρονοδιάγραμμα

Η συνολική διάρκεια της σύμβασης ορίζεται σε **40 ημέρες** και νοείται το χρονικό διάστημα από την ημερομηνία υπογραφής της σύμβασης έως την υποβολή του τελευταίου παραδοτέου σύμφωνα με το αναλυτικό χρονοδιάγραμμα που παρατίθεται στη συνέχεια.

ΦΑΣΗ	**ΤΙΤΛΟΣ ΦΑΣΗΣ**	**ΕΒΔΟΜΑΔΑ ΥΛΟΠΟΙΗΣΗΣ**						
		1	2	3	4	5	6	7
ΦΑΣΗ 1	Μελέτη Εφαρμογής							
ΦΑΣΗ 2	Ανάπτυξη & Παραμετροποίηση							
ΦΑΣΗ 3	Εκπαίδευση							
ΦΑΣΗ 4	Πιλοτική Λειτουργία							

ΠΑΡΑΡΤΗΜΑ 3
Κατάρτιση Προσφοράς

3.1.Προϋποθέσεις συμμετοχής

Προσφορά που αποκλίνει από τις τεχνικές προδιαγραφές και τις προϋποθέσεις της παρούσας πρόσκλησης και των παραρτημάτων αυτής θα κριθεί ως απαράδεκτη και θα απορριφθεί.

3.2. Δικαιολογητικά Συμμετοχής

Τα στοιχεία και δικαιολογητικά για την συμμετοχή του προσφέροντος στη διαδικασία περιλαμβάνουν επί ποινή αποκλεισμού τα στοιχεία που περιγράφονται ακολούθως:

1.Αντίγραφο ασφαλιστικής ενημερότητας για συμμετοχή σε διαγωνισμούς του δημοσίου.

2.Αντίγραφο φορολογικής ενημερότητας για κάθε νόμιμη χρήση.

3.Πιστοποιητικό ΓΕΜΗ ή αναγνωρισμένου αντίστοιχου φορέα σε ισχύ και πιστοποιητικό ισχύουσας εκπροσώπησης από το ΓΕΜΗ, με ημερομηνία έκδοσης είτε τριάντα (30) εργάσιμων ημερών πριν την υποβολή του είτε μεταγενέστερης της κοινοποίησης της παρούσας πρόσκλησης.

4.Στοιχεία σύστασης και εκπροσώπησης εταιρείας με τις πιθανές τροποποιήσεις ή για φυσικά πρόσωπα Βεβαίωση Έναρξης Εργασιών Φυσικού Προσώπου Επιτηδευματία.

5.Απόσπασμα/τα ποινικού μητρώου των εταίρων ή των μελών του Δ.Σ. - ή του Φυσικού Προσώπου, με ημερομηνία έκδοσης έως τρεις (3) μήνες πριν από την υποβολή τους. Σε περίπτωση αναμονής έκδοσης τους, δύναται να προσκομιστεί υπεύθυνη δήλωση του άρθ. 8 παρ. 4 του ν.1599/1986, στην οποία να δηλώνεται ότι ο ανάδοχος δεν εμπίπτει στις διατάξεις της παρ.1 άρθρου 73 του ν.4412/2016. Στην περίπτωση κατάθεσης υπεύθυνης δήλωσης, εντός 10 ημερών από την υπογραφή της σύμβασης, θα πρέπει να προσκομιστούν τα ανωτέρω αναφερόμενα αποσπάσματα ποινικού μητρώου.

6.Υπεύθυνη δήλωση υπογεγραμμένη απ' το νόμιμο εκπρόσωπο της εταιρείας, στην οποία θα αναφέρεται ότι δεν έχει επιβληθεί σε βάρος του αναδόχου η οριζόντια ρήτρα αποκλεισμού σύμφωνα με τις διατάξεις του άρθρου 74 του ν.4412/2016.

7.Υπεύθυνη δήλωση υπογεγραμμένη από το νόμιμο εκπρόσωπο της εταιρείας, στην οποία θα δηλώνεται ότι αποδέχεται πλήρως και ανεπιφύλακτα όλους τους όρους της παρούσας πρόσκλησης.

8.Υπεύθυνη δήλωση υπογεγραμμένη απ' το νόμιμο εκπρόσωπο της εταιρείας με το ακόλουθο περιεχόμενο: «Δηλώνω υπεύθυνα ότι δεν υπάρχει ρωσική συμμετοχή στην εταιρεία που εκπροσωπώ, σύμφωνα με τους περιορισμούς που περιλαμβάνονται στο άρθρο 5ια του κανονισμού του Συμβουλίου (ΕΕ) αριθ. 833/2014 της 31ης Ιουλίου 2014 σχετικά με περιοριστικά μέτρα λόγω των ενεργειών της Ρωσίας που αποσταθεροποιούν την κατάσταση στην Ουκρανία, όπως τροποποιήθηκε από τον με αριθ. 2022/578 Κανονισμό του Συμβουλίου (ΕΕ) της 8ης Απριλίου 2022. Συγκεκριμένα δηλώνω ότι : (α) ο Ανάδοχος που εκπροσωπώ (και καμία από τις εταιρείες που εκπροσωπούν μέλη της κοινοπραξίας μας) δεν είναι Ρώσος υπήκοος, ούτε φυσικό ή νομικό πρόσωπο, οντότητα ή φορέας εγκατεστημένος στη Ρωσία· (β) ο Ανάδοχος που εκπροσωπώ (και καμία από τις εταιρείες που εκπροσωπούν μέλη της κοινοπραξίας μας) δεν είναι νομικό πρόσωπο, οντότητα ή φορέας του οποίου τα δικαιώματα ιδιοκτησίας κατέχει άμεσα ή έμμεσα σε ποσοστό άνω του πενήντα τοις εκατό (50%) οντότητα

αναφερόμενη στο στοιχείο α) της παρούσας παραγράφου· (γ) ούτε ο υπεύθυνα δηλώνων ούτε η εταιρεία που εκπροσωπώ δεν είμαστε φυσικό ή νομικό πρόσωπο, οντότητα ή όργανο που ενεργεί εξ ονόματος ή κατ' εντολή οντότητας που αναφέρεται στο σημείο(α) ή (β) παραπάνω, (δ) δεν υπάρχει συμμετοχή φορέων και οντοτήτων που απαριθμούνται στα ανωτέρω στοιχεία α) έως γ), άνω του 10 % της αξίας της σύμβασης των υπεργολάβων, προμηθευτών ή φορέων στις ικανότητες των οποίων να στηρίζεται ο Ανάδοχος τον οποίον εκπροσωπώ».
Οι υπεύθυνες δηλώσεις γίνονται αποδεκτές εφόσον έχουν συνταχθεί μετά την κοινοποίηση της παρούσας πρόσκλησης (άρθρο 80 παρ.12 του ν.4412/2016, όπως προστέθηκε με την παρ.7αδ του άρθρου 43 του ν.4605/2019).
Τα ανωτέρω πιστοποιητικά γίνονται αποδεκτά εφόσον είναι εν ισχύ κατά το χρόνο υποβολής τους, άλλως στην περίπτωση που δεν αναφέρεται ο χρόνος ισχύος, εφόσον έχουν εκδοθεί έως τρεις (3) μήνες πριν από την υποβολή τους (άρθρο 80 παρ.12 του ν.4412/2016, όπως προστέθηκε με την παρ.7αδ του άρθρου 43 του ν.4605/2019).

3.3.Περιεχόμενα Φακέλου «Προσφορά» / Τρόπος σύνταξης και υποβολής οικονομικών προσφορών

Η Οικονομική Προσφορά πρέπει να περιλαμβάνει **:**

Προσφερόμενη τιμή για την παροχή υπηρεσιών ανάπτυξης νέου Ολοκληρωμένου Πληροφοριακού Σύστηματος (ΟΠΣ) Ψηφιακής Προ-έγκρισης Αιτημάτων Ληξιαρχικών Μητρώων.

Στην ανωτέρω τιμή συμπεριλαμβάνονται οι υπέρ τρίτων κρατήσεις και κάθε άλλη επιβάρυνση, σύμφωνα με την κείμενη νομοθεσία, για την προμήθεια των αγαθών στον τόπο και με τον τρόπο που θα προβλέπεται στα έγγραφα της σύμβασης.
Η προσφερόμενη τιμή είναι σταθερή καθ' όλη τη διάρκεια της σύμβασης και δεν αναπροσαρμόζεται.
Ως απαράδεκτη θα απορριφθεί η προσφορά εφόσον:
α) δε δίνεται τιμή σε ΕΥΡΩ ή καθορίζεται σχέση ΕΥΡΩ προς ξένο νόμισμα,
β) δεν προκύπτει με σαφήνεια η προσφερόμενη τιμή, με την επιφύλαξη του άρθρου 102 του ν. 4412/2016
γ) η συνολική τιμή άνευ Φ.Π.Α υπερβαίνει τον συνολικό προϋπολογισμό άνευ Φ.Π.Α της παρούσας πρόσκλησης.

3.4.Χρόνος ισχύος της προσφοράς

Η προσφορά ισχύει και δεσμεύει τον προσκαλούμενο οικονομικό φορέα για τριάντα (30) μέρες από την κατάθεσή της. Προσφορά που αναφέρει χρόνο ισχύος μικρότερο των τριάντα (30) ημερών απορρίπτεται ως απαράδεκτη. Η αναγραφή του χρόνου ισχύος της προσφοράς είναι <u>υποχρεωτική.</u>
Η ισχύς της προσφοράς μπορεί να παρατείνεται εγγράφως, εφόσον τούτο ζητηθεί από την Αναθέτουσα Αρχή, πριν από τη λήξη της σύμφωνα με τα οριζόμενα στο άρθρο 72 παρ. 1α του ν. 4412/2016, κατ' ανώτατο όριο για χρονικό διάστημα ίσο με την προβλεπόμενη ως άνω αρχική διάρκεια.

ΠΑΡΑΡΤΗΜΑ 4

Οικονομικά Στοιχεία του Έργου – Τρόπος Πληρωμής

Η προσφορά υποβάλλεται για το σύνολο των ζητούμενων υπηρεσιών, επί ποινή αποκλεισμού, για λόγους συμβατότητας, και εφαρμογής ενιαίων πρακτικών διαχείρισης της προμήθειας.

Φορέας χρηματοδότησης της παρούσας σύμβασης είναι το Υπουργείο Εσωτερικών. Η παρούσα σύμβαση βαρύνει τις πιστώσεις του τακτικού προϋπολογισμού εξόδων του Υπουργείου Εσωτερικών, και συγκεκριμένα του **ΑΛΕ 2420989001 «Έξοδα για λοιπές υπηρεσίες», του Ε.Φ. 1007-206,** οικονομικού έτους 2025, για έως το ποσό των **εβδομήντα τεσσάρων χιλιάδων τετρακοσίων ευρώ (74.400,00€)** συμπεριλαμβανομένου του Φ.Π.Α 24%.

Η πληρωμή της αναδόχου εταιρείας θα πραγματοποιηθεί με την έκδοση χρηματικού εντάλματος πληρωμής στο όνομά της. Η πληρωμή θα πραγματοποιηθεί μετά την έκδοση πρωτοκόλλου παραλαβής των σχετικών παραδοτέων από την αρμόδια επιτροπή παραλαβής και την έκδοση του αντίστοιχου ηλεκτρονικού τιμολογίου.

ΠΑΡΑΡΤΗΜΑ 5

Προστασία προσωπικών δεδομένων - Υποχρέωση εχεμύθειας και εμπιστευτικότητας

Η Αναθέτουσα Αρχή ενημερώνει, υπό την ιδιότητά της ως υπεύθυνη επεξεργασίας, το φυσικό πρόσωπο που υπογράφει την προσφορά ως Προσφέρων ή ως Νόμιμος Εκπρόσωπος Προσφέροντος, ότι το ίδιο ή και τρίτοι, κατ' εντολή και για λογαριασμό του, θα επεξεργάζονται τα ακόλουθα δεδομένα ως εξής:

I. Αντικείμενο επεξεργασίας είναι τα δεδομένα προσωπικού χαρακτήρα που περιέχονται στους φακέλους της προσφοράς και τα αποδεικτικά μέσα τα οποία υποβάλλονται στην Αναθέτουσα Αρχή, στο πλαίσιο του παρόντος Διαγωνισμού, από το φυσικό πρόσωπο το οποίο είναι το ίδιο Προσφέρων ή Νόμιμος Εκπρόσωπος Προσφέροντος.

II. Σκοπός της επεξεργασίας είναι η αξιολόγηση του Φακέλου Προσφοράς, η ανάθεση της Σύμβασης, η προάσπιση των δικαιωμάτων της Αναθέτουσας Αρχής, η εκπλήρωση των εκ του νόμου υποχρεώσεων της Αναθέτουσας Αρχής και η εν γένει ασφάλεια και προστασία των συναλλαγών. Τα δεδομένα ταυτοπροσωπίας και επικοινωνίας θα χρησιμοποιηθούν από την Αναθέτουσα Αρχή και για την ενημέρωση των Προσφερόντων σχετικά με την αξιολόγηση των προσφορών.

III. Αποδέκτες των ανωτέρω (υπό I) δεδομένων στους οποίους κοινοποιούνται είναι:

(α) Ο φορέας στον οποίο η Αναθέτουσα Αρχή αναθέτει την εκτέλεση συγκεκριμένων ενεργειών για λογαριασμό της, δηλαδή οι Σύμβουλοι, τα υπηρεσιακά στελέχη, μέλη Επιτροπών Αξιολόγησης, Χειριστές του Ηλεκτρονικού Διαγωνισμού και λοιποί εν γένει προστηθέντες της, υπό τον όρο της τήρησης σε κάθε περίπτωση του απορρήτου.

(β) Το Δημόσιο, άλλοι δημόσιοι φορείς ή δικαστικές αρχές ή άλλες αρχές ή δικαιοδοτικά

όργανα, στο πλαίσιο των αρμοδιοτήτων τους.
IV. Τα δεδομένα θα τηρούνται για χρονικό διάστημα ίσο με τη διάρκεια της εκτέλεσης της σύμβασης, και μετά τη λήξη αυτής για χρονικό διάστημα πέντε ετών, για μελλοντικούς φορολογικούς-δημοσιονομικούς ή ελέγχους χρηματοδοτών ή άλλους προβλεπόμενους ελέγχους από την κείμενη νομοθεσία, εκτός εάν η νομοθεσία προβλέπει διαφορετική περίοδο διατήρησης. Σε περίπτωση εκκρεμοδικίας αναφορικά με δημόσια σύμβαση τα δεδομένα τηρούνται μέχρι το πέρας της εκκρεμοδικίας. Μετά τη λήξη των ανωτέρω περιόδων, τα προσωπικά δεδομένα θα καταστρέφονται.
V. Το φυσικό πρόσωπο που είναι είτε Προσφέρων είτε Νόμιμος Εκπρόσωπος του Προσφέροντος, μπορεί να ασκεί κάθε νόμιμο δικαίωμά του σχετικά με τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, απευθυνόμενο στον υπεύθυνο προστασίας προσωπικών δεδομένων της Αναθέτουσας Αρχής, dpo@ypes.gr
VI. Η Αναθέτουσα Αρχή έχει υποχρέωση να λαμβάνει κάθε εύλογο μέτρο για τη διασφάλιση του απόρρητου και της ασφάλειας της επεξεργασίας των δεδομένων και της προστασίας τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση από οποιονδήποτε και κάθε άλλης μορφή αθέμιτη επεξεργασία.

Ο υποψήφιος Ανάδοχος υποχρεούται, τόσο κατά τη διάρκεια ισχύος της υπογραφείσας σύμβασης, όσο και μετά τη λήξη ή καταγγελία της, να χρησιμοποιεί τα στοιχεία και τις πληροφορίες που θα του γνωστοποιηθούν ή που θα περιέλθουν σε γνώση του μόνο για το σκοπό της εκπλήρωσης των υποχρεώσεών του που απορρέουν από την υπογραφείσα σύμβαση και να μην τα γνωστοποιεί παρά μόνο σε πρόσωπα που εμπλέκονται άμεσα στην εκπλήρωση των ανωτέρω υποχρεώσεων και είναι απαραίτητο να γνωρίζουν τα εν λόγω στοιχεία, τα οποία με δική του ευθύνη εποπτεύει ως προς την εφαρμογή από το μέρος τους των υποχρεώσεων του αναδόχου.

Ο υποψήφιος Ανάδοχος αναλαμβάνει την υποχρέωση να τηρεί τις υποχρεώσεις που απορρέουν από τον ν.4624/2019, όπως ισχύει, καθώς και από τις διατάξεις του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός Προστασίας Δεδομένων/General Data Protection Regulation– GDPR).

Ο υποψήφιος Ανάδοχος υποχρεούται να ακολουθεί κάθε επιπλέον έγγραφη οδηγία ή ενημέρωση για την ασφάλεια των πληροφοριών που θα δοθεί από την Αναθέτουσα Αρχή. Επίσης θέτει στη διάθεση της αρμόδιας Οργανικής Μονάδας της Αναθέτουσας Αρχής κάθε απαραίτητη πληροφορία σχετικά με τα μέτρα που λαμβάνει για την τήρηση των υποχρεώσεων που περιγράφονται στο άρθρο αυτό, επιτρέπει και διευκολύνει τους ελέγχους σε οποιονδήποτε προσωπικό υπολογιστή ή φορητό αποθηκευτικό μέσο του που βρίσκεται στην υπηρεσία για λόγους ασφάλειας και προστασίας των πληροφοριακών συστημάτων και των δεδομένων τους.

Ο υποψήφιος Ανάδοχος αναλαμβάνει την υποχρέωση να διασφαλίζει όλα τα πληροφοριακά στοιχεία στους χώρους, που θα προσδιορίζονται στη Σύμβαση και στους ανθρώπους, που ασχολούνται με το Έργο, αποκλειόμενης της διαφυγής, διαρροής ή μεταφοράς σε άλλα άτομα, χώρους ή εταιρείες.

Ο υποψήφιος Ανάδοχος υποχρεούται να ενημερώνει την Αναθέτουσα Αρχή για τα λαμβανόμενα, στην κατεύθυνση αυτή μέτρα. Εάν οποιαδήποτε στιγμή, υπάρξουν ενδείξεις ότι

έχουν διαρρεύσει ή πρόκειται να διαρρεύσουν πληροφορίες, ο Ανάδοχος υποχρεούται να ενημερώνει άμεσα, το αργότερο εντός είκοσι τεσσάρων (24) ωρών, την αρμόδια Οργανική Μονάδα της Αναθέτουσας Αρχής καθώς και τον Υπεύθυνο Προστασίας Δεδομένων της Αναθέτουσας Αρχής, dpo@ypes.gr. Ειδικότερα, ο Ανάδοχος υποχρεούται, ως εκτελών την επεξεργασία δεδομένων προσωπικού χαρακτήρα, να εκτελεί την εργασία κατ΄ εντολή της Αναθέτουσας Αρχής, και να βαρύνεται αναλόγως με όλες τις υποχρεώσεις της Αναθέτουσας Αρχής, που προκύπτουν από τις διατάξεις της Ελληνικής και Κοινοτικής Νομοθεσίας για την προστασία δεδομένων προσωπικού χαρακτήρα όπως αυτή ισχύει. Σε κάθε περίπτωση παράβασης των ως άνω υποχρεώσεων του Αναδόχου, πέραν από τα ειδικά προβλεπόμενα στη διακήρυξη ή τη Σύμβαση, που θα υπογραφεί ισχύουν και οι κυρώσεις του ισχύοντος νομικού πλαισίου.

Σε περίπτωση που υπάρξει διαρροή πληροφοριών, η οποία οφείλεται σε πράξη ή παράλειψη του Αναδόχου ή/και των μελών της Ομάδας Έργου, η Αναθέτουσα Αρχή διατηρεί το δικαίωμα να κάνει χρήση των διατάξεων «περί πνευματικής ιδιοκτησίας», να κοστολογήσει και να απαιτήσει πληρωμή για όλες τις άμεσες και έμμεσες, θετικές ή αποθετικές ζημιές, που θα έχει κατά περίπτωση υποστεί, καθώς επίσης και να προβεί στην καταγγελία της Σύμβασης, εξαιτίας υπαιτιότητας του Αναδόχου, κηρύσσοντάς τον έκπτωτο .