@ΣΗΔΕ ΙΡΙΔΑ
67f637e6a71278c1409c6387
ΑΠ:22045
Υπογραφή: 24/04/25 11:59
Διανομή: 24/04/25 13:16

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΟΙΚΟΝΟΜΙΚΩΝ ΥΠΗΡΕΣΙΩΝ
& ΔΙΟΙΚΗΤΙΚΗΣ ΥΠΟΣΤΗΡΙΞΗΣ
ΔΙΕΥΘΥΝΣΗ ΠΡΟΜΗΘΕΙΩΝ & ΥΠΟΔΟΜΩΝ
ΤΜΗΜΑ ΠΡΟΜΗΘΕΙΩΝ
Πληροφορίες: Ε. Ασπρουλάκη
Ταχ. Δ/νση: Σταδίου 31
Ταχ. Κώδικας: 101 83 ΑΘΗΝΑ
Τηλέφωνο: 213 136 1654
e-mail: e.asproulaki@ypes.gr

Αθήνα, 24 -04-2025
Αριθ. Πρωτ.: 22045

**Προς:** MIRKWOOD E.E
info@mirkwood-systems.com

**ΘΕΜΑ: Πρόσκληση εκδήλωσης ενδιαφέροντος για κατάθεση οικονομικής προσφοράς για την υλοποίηση έργου που αφορά στη δημιουργία νέου Πληροφοριακού Συστήματος (ΠΣ) Διαχείρισης Πληρωμών Προγραμμάτων ΥΠ.ΕΣ.**

Το Υπουργείο Εσωτερικών, προκειμένου να καλυφθεί η δαπάνη που αφορά τη δημιουργία νέου Πληροφοριακού Συστήματος (ΠΣ) Διαχείρισης Πληρωμών Προγραμμάτων ΥΠ.ΕΣ., με σκοπό την υποστήριξη της διαχείρισης οικονομικών στοιχείων αιτημάτων και διεκπεραίωσης πληρωμών Ο.Τ.Α. των επιλεγμένων Αναπτυξιακών Προγραμμάτων του ΥΠ.ΕΣ., θα προβεί στη σύναψη σχετικής σύμβασης.
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 άρθρων 118 και της παρ. 3 του άρθρου 120., καθώς και τη με αρ. πρωτ. 9486 ΕΞ 2025/24.03.2025 Διαπιστωτική Πράξη για την κατά παρέκκλιση της παρ.1 του άρθρου 118 του ν.4412/2016 προσφυγή στη διαδικασία της απευθείας ανάθεσης για έργα Τεχνολογιών Πληροφορικής και Επικοινωνιών (Τ.Π.Ε.)
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
- Παράρτημα 5 : Εγγυητική επιστολή καλής εκτέλεσης
- Παράρτημα 6: Χρονική διάρκεια σύμβασης
- Παράρτημα 7 : Υποχρέωση εχεμύθειας και εμπιστευτικότητας – Προστασία προσωπικών δεδομένων

**Ο ΥΠΗΡΕΣΙΑΚΟΣ ΓΡΑΜΜΑΤΕΑΣ**

**ΠΑΝΤΕΛΗΣ ΤΑΓΚΑΛΑΚΗΣ**

**Εσωτερική Διανομή:**

1. Γραφείο Γενικού Γραμματέα Αυτοδιοίκησης και Αποκέντρωσης
2. Γραφείο Υπηρεσιακού Γραμματέα
3. Διεύθυνση Οικονομικής και Αναπτυξιακής Πολιτικής
4. Γραφείο Γενικού Διευθυντή Εσωτερικών & Ηλεκτρονικής Διακυβέρνησης
5. Διεύθυνση Προμηθειών και Υποδομών

## ΠΑΡΑΡΤΗΜΑ 1

### Γενικά Στοιχεία Πρόσκλησης

| | |
|---|---|
| ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ | ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ (τ. Εσωτερικών) |
| ΜΟΝΑΔΑ ΦΟΡΕΑ | ΔΙΕΥΘΥΝΣΗ ΠΡΟΜΗΘΕΙΩΝ & ΥΠΟΔΟΜΩΝ<br>ΤΜΗΜΑ ΠΡΟΜΗΘΕΙΩΝ |
| ΕΙΔΟΣ ΣΥΜΒΑΣΗΣ | Απευθείας ανάθεση βάσει των άρθρων 118 και 120, παρ. 3 του ν.4412/2016, όπως έχει τροποποιηθεί και ισχύει, καθώς και τη με αρ. πρωτ. 9486 ΕΞ 2025/24.03.2025 Διαπιστωτική Πράξη για την κατά παρέκκλιση της παρ.1 του άρθρου 118 του ν.4412/2016 προσφυγή στη διαδικασία της απευθείας ανάθεσης για έργα Τεχνολογιών Πληροφορικής και Επικοινωνιών (Τ.Π.Ε.) |
| ΠΕΡΙΓΡΑΦΗ ΘΕΜΑΤΟΣ-<br>ΠΡΟΣΚΑΛΟΥΜΕΝΟΣ ΟΙΚΟΝΟΜΙΚΟΣ ΦΟΡΕΑΣ | Δημιουργία νέου Πληροφοριακού Συστήματος (ΠΣ) Διαχείρισης Πληρωμών Προγραμμάτων του Υπουργείου Εσωτερικών, σύμφωνα με τα ΠΑΡΑΡΤΗΜΑΤΑ τα οποία αποτελούν αναπόσπαστα μέρη της παρούσας<br><br>Για την σύναψη της σχετικής σύμβασης, το Υπουργείο Εσωτερικών προσκαλεί την εταιρεία με την επωνυμία **«MIRKWOOD ΕΕ»** που εδρεύει στον **Δήμο Γαλατσίου, Δρυάδων 50, Γαλάτσι, Τ.Κ. 11146**, ΑΦΜ: 802716189, **ΔΟΥ: ΚΕΦΟΔΕ Αττικής** , να καταθέσει οικονομική και τεχνική προσφορά, βάσει των ειδικών τεχνικών όρων και των προδιαγραφών των παρακάτω παραρτημάτων τα οποία αποτελούν **αναπόσπαστο μέρος** της παρούσας πρόσκλησης.<br><br>**Η μη τήρηση των ανωτέρω, συνεπάγεται την απόρριψη της προσφοράς.**<br><br>**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.**<br><br>Οι προδιαγραφές της εν λόγω προμήθειας αναφέρονται στα Παραρτήματα 1, 2, 3, 4, 5,6 και 7 τα οποία αποτελούν αναπόσπαστο μέρος της παρούσας **(ΕΠΙ ΠΟΙΝΗ ΑΠΟΚΛΕΙΣΜΟΥ)** |
| ΚΡΙΤΗΡΙΑ ΑΝΑΘΕΣΗΣ : | Η πλέον συμφέρουσα, από οικονομική άποψη, προσφορά βάσει τιμής. |
| ΕΚΤΙΜΩΜΕΝΟ ΚΟΣΤΟΣ | Ποσό άνευ Φ.Π.Α.**: 60.000,00 €**<br>Ποσό συμπεριλαμβανομένου Φ.Π.Α 24% : **74.400,00 €** |
| ΚΩΔΙΚΟΣ ΠΡΟΫΠΟΛΟΓΙΣΜΟΥ ΦΟΡΕΑ | Προϋπολογισμός Δημοσίων Επενδύσεων (ΠΔΕ) και συγκεκριμένα του ΚΩΔ. **ΣΑ ΝΑ655** με κωδικό εναρίθμου **2024ΝΑ65500000** |
| ΕΓΓΥΗΤΙΚΗ ΕΠΙΣΤΟΛΗ | Για την υπογραφή της σύμβασης απαιτείται η παροχή εγγύησης καλής εκτέλεσης, σύμφωνα με το άρθρο 72 παρ. 4 του ν. 4412/2016, το ύψος της οποίας ανέρχεται σε ποσοστό **4%** επί της εκτιμώμενης αξίας της σύμβασης, ή του τμήματος αυτής, ήτοι στο ποσό των **δύο χιλιάδων τετρακοσίων ευρώ** (**2.400,00€)** και η οποία κατατίθεται μέχρι και την υπογραφή του συμφωνητικού. |
| ΔΙΑΡΚΕΙΑ ΣΥΜΒΑΣΗΣ | Η διάρκεια της σύμβασης εκτείνεται σε τέσσερις (4) μήνες από την υπογραφής της. |

| | |
|---|---|
| CPV | 72514200-3 Υπηρεσίες διαχείρισης εγκαταστάσεων για την ανάπτυξη συστημάτων πληροφορικής |
| ΠΑΡΑΚΡΑΤΗΣΗ ΦΟΡΟΥ ΕΠΙ ΤΗΣ ΚΑΘΑΡΗΣ ΣΥΜΒΑΤΙΚΗΣ ΑΞΙΑΣ | • **Φόρος**: 8% (οκτώ τοις εκατό) για την παροχή υπηρεσίας σύμφωνα με το άρθρο 64 του ν.4172/2013, όπως τροποποιήθηκε και ισχύει & όσων άλλων κατά νόμο κρατήσεων βρίσκονται σε ισχύ κατά την ημερομηνία υπογραφής της σύμβασης.<br>• **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 –<br><br>ΕΓΚΡΙΣΗ ΠΙΣΤΩΣΗΣ/ΒΕΒΑΙΩΣΗ ΥΠΑΡΞΗΣ ΔΙΑΘΕΣΙΜΩΝ ΠΟΡΩΝ | Υπ' αρ. 9724/21-02-2025 (ΑΔΑΜ: 25REQ016594844)<br><br>Υπ' αρ. 19054/27-04-2025 (ΑΔΑΜ: 25REQ016616773) |
| ΠΡΟΘΕΣΜΙΑ ΚΑΤΑΘΕΣΗΣ ΠΡΟΣΦΟΡΑΣ | Έως την **Τρίτη 29 Απριλίου 2025** και ώρα **12:00** |
| ΤΑΧ. Δ/ΝΣΗ ΑΝΑΘΕΤΟΥΣΑΣ ΑΡΧΗΣ ΚΑΙ ΤΟΠΟΣ ΚΑΤΑΘΕΣΗΣ ΠΡΟΣΦΟΡΑΣ | Υπουργείο Εσωτερικών<br>Δ/νση Προμηθειών & Υποδομών<br>Τμήμα Προμηθειών<br>Υπόψη Ε. Ασπρουλάκη<br>Σταδίου 31, 4ος όροφος, Τ.Κ. 101 83 Αθήνα<br>E-mail : e.asproulaki@ypes.gr<br>Τηλέφωνο : 2131361654 |
| 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).<br>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<br>ΑΦΜ: 090056250<br>ΔΟΥ: Α' ΑΘΗΝΩΝ<br><br>ΚΩΔΙΚΟΣ ΑΑΗΤ: 1007.0000000000.0001<br><br>ΑΔΑΜ ΑΝΑΛΗΨΗΣ: 25REQ016616773 |

| | |
|---|---|
| ΚΑΝΟΝΕΣ ΔΗΜΟΣΙΟΤΗΤΑΣ | Η παρούσα ανακοίνωση αναρτάται:<br>α) στην ιστοσελίδα του ΥΠΕΣ www.ypes.gr,<br>β) στο Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ) www.eprocurement.gov.gr |

## ΠΑΡΑΡΤΗΜΑ 2

### Τεχνικές Προδιαγραφές

Έργο του Αναδόχου είναι η δημιουργία νέου Πληροφοριακού Συστήματος (ΠΣ) Διαχείρισης ΤΠΑ ΥΠΕΣ.
Το αντικείμενο του έργου που πρέπει να υλοποιηθεί αφορά την ανάπτυξη και λειτουργία νέου Πληροφοριακού Συστήματος (ΠΣ) Διαχείρισης Πληρωμών Προγραμμάτων ΥΠΕΣ, το οποίο θα υποστηρίξει τη διαχείριση οικονομικών στοιχείων αιτημάτων και διεκπεραίωσης πληρωμών Ο.Τ.Α. των επιλεγμένων Αναπτυξιακών Προγραμμάτων του ΥΠ.ΕΣ., παρέχοντας όπου απαιτείται την απαραίτητη διαλειτουργικότητα στα υφιστάμενα Συστήματα των εξής Προγραμμάτων: «Αντώνης Τρίτσης», «ΦΙΛΟΔΗΜΟΣ ΙΙ», «Βελτίωση οδικής ασφάλειας στο εθνικό και επαρχιακό Οδικό Δίκτυο» του ΤΑΑ, «ΤΠΑ ΥΠΕΣ», «Ειδικό Πρόγραμμα Φυσικών Καταστροφών».

Βάσει όλων των κατωτέρω περιγραφόμενων τεχνικών προδιαγραφών του ΠΑΡΑΡΤΗΜΑΤΟΣ 2 της παρούσας πρόσκλησης, ο Προσφέρων υποχρεούται να υποβάλλει – με ΠΟΙΝΗ ΑΠΟΚΛΕΙΣΜΟΥ – στον (υπο)φάκελο «Τεχνική Προσφορά», συμπληρωμένο, μονογραμμένο σε κάθε σελίδα του και υπογεγραμμένο πίνακα συμμόρφωσης – τεχνική περιγραφή για τον οποίο υποβάλλει προσφορά.

### Α) Λειτουργικές Απαιτήσεις Έργου

1. Υποβολή Στοιχείων Αιτημάτων Πληρωμών από Ο.Τ.Α.: Θα παρέχεται η δυνατότητα καταχώρησης των απαραίτητων στοιχείων αιτημάτων πληρωμής από τους πιστοποιημένους Υπαλλήλους Ο.Τ.Α. .
2. Επισκόπηση συγκεντρωτικών στοιχείων Αιτημάτων Πληρωμών από Ο.Τ.Α.: Θα παρέχεται η δυνατότητα επισκόπησης των προηγούμενων αιτημάτων πληρωμών του Ο.Τ.Α., με λεπτομέρειες σχετικά με την κατάσταση κάθε αιτήματος (π.χ. καταχωρημένο, υποβληθέν, σε επεξεργασία, πληρωμένο).
3. Διαχείριση Αιτημάτων Πληρωμής Ο.Τ.Α. από ΥΠ.ΕΣ.: Θα παρέχεται η δυνατότητα διαχείρισης αιτημάτων πληρωμών από τους πιστοποιημένους Υπαλλήλους του ΥΠ.ΕΣ. περιλαμβάνοντας :
   - Την αλλαγή της κατάστασης ενός αιτήματος από "Υποβληθέν Αίτημα" σε "Αίτημα σε Επεξεργασία" και στη συνέχεια σε "Οριστικοποίηση Πληρωμής".
   - Τη δυνατότητα προβολής συγκεντρωτικών στοιχείων ανά Πρόγραμμα, είτε για έναν είτε για πολλούς Ο.Τ.Α., βάσει των δικαιωμάτων που παρέχονται στον ρόλο του εκάστοτε Χρήστη.
4. Ενοποίηση δεδομένων εντάξεων Έργων: Θα παρέχεται η δυνατότητα προβολής ενοποιημένων δεδομένων σε οθόνες που περιλαμβάνουν στοιχεία αίτησης ένταξης, οριστικής ένταξης και υπόλοιπων στοιχείων, τα οποία αντλούνται από άλλα υφιστάμενα σε λειτουργία Συστήματα.

   Ειδικότερα :

- Στοιχεία από ΕΕΤΑΑ, ΟΠΣ ΕΠΑ, Ταμείο Παρακαταθηκών και Δανείων (e- Loans), e-ΠΔΕ.
- Στατική απεικόνιση στοιχείων Προγράμματος ΚΑΠ (Κεντρικοί Αυτοτελείς Πόροι)
- μέσω λήψης προκαθορισμένου και προσυμπληρωμένου αρχείου από την αρμόδια Διεύθυνση ΥΠ.ΕΣ. .

5. Αναφορές, γραφήματα και στατιστικά στοιχεία για την Πολιτική Ηγεσία του ΥΠ.ΕΣ.Η Ενότητα αυτή περιλαμβάνει :

- Εξειδικευμένες αναφορές που παρουσιάζουν συγκεντρωτικά δεδομένα ανά Φορέα,Πρόγραμμα, γεωγραφική περιοχή (Περιφέρεια, Νομός, Δήμος) και επιλεγμένη χρονική περίοδο.
- Διαδραστικές απεικονίσεις που βοηθούν στη λήψη στρατηγικών αποφάσεων για την πορεία των σχετικών Προγραμμάτων.

6 . Διαχείριση χρηστών και ρόλων

- Καθορισμός ρόλων χρηστών (π.χ. Υπάλληλοι ΟΤΑ, Υπάλληλοι ΥΠ.ΕΣ., Διαχειριστές) με διαβαθμισμένη πρόσβαση.
- Διαχείριση δικαιωμάτων ανά ρόλο, ώστε κάθε χρήστης να έχει πρόσβαση μόνο στις αντίστοιχες λειτουργίες και δεδομένα.
- Ύπαρξη διαχειριστικού περιβάλλοντος δημιουργίας, ενεργοποίησης, απενεργοποίησης κ.λ.π χρηστών και δικαιωμάτων.

7. Ειδοποιήσεις και ιστορικό δράσεων:

- Αυτόματες ειδοποιήσεις μέσω email, sms ή/και ενσωματωμένων μηνυμάτων εντός του συστήματος όταν αλλάζει η κατάσταση ενός αιτήματος πληρωμής ή όταν συμβαίνει κάποιο άλλο γεγονός για το οποίο ο χρήστης πρέπει να λαμβάνει γνώση.
- Καταγραφή ιστορικού ενεργειών για κάθε αίτημα (π.χ. ποιος χρήστης έκανε αλλαγές και πότε).

8. Επαλήθευση και έλεγχος καταχωρήσεων δεδομένων

- Έλεγχος πληρότητας των αιτήσεων πληρωμής πριν από την υποβολή.
- Αυτόματη διασταύρωση στοιχείων με άλλα συστήματα μέσω web services, όπου είναι εφικτό.
- Ειδοποιήσεις για μη έγκυρα ή ελλιπή δεδομένα.

**<u>Β) Τεχνικές Προδιαγραφές – Απαιτήσεις αρχιτεκτονικής</u>**

1. **Αρχιτεκτονική και Υποδομή**

- Web-based σύστημα με responsive design για πρόσβαση από desktop και mobile συσκευές.
- Εγκατάσταση στο κυβερνητικό νέφος.
- Υιοθέτηση κρατικής υποδομής αυθεντικοποίησης κάνοντας χρήση κωδικών δημόσιας

διοίκησης.

- Συμμόρφωση με τα πρότυπα προσβασιμότητας για ΑΜΕΑ (WCAG 2.1).
- Σχεδιασμός με multi-tier αρχιτεκτονική με σκοπό την μέγιστη δυνατή επεκτασιμότητα του συστήματος όταν παραστεί η ανάγκη.

2. **Διαλειτουργικότητα με Άλλα Συστήματα**

- Διασύνδεση με τα εμπλεκόμενα πληροφοριακά συστήματα (ΕΕΤΑΑ, ΟΠΣ ΕΠΑ, e-ΠΔΕ, Ταμείο Παρακαταθηκών και Δανείων) μέσω REST APIs που ενδεχομένως προσφέρονται από τους εν λόγω φορείς. (θα πρέπει να πραγματοποιηθεί επικοινωνία με τους εμπλεκόμενους φορείς για διερεύνηση των δυνατοτήτων διαλειτουργικότητας)
- Εξαγωγή δεδομένων σε δομημένες μορφές (CSV, XML, JSON) για χρήση από τρίτα συστήματα και παροχή δεδομένων μέσω REST APIs για την κάλυψη ενδεχόμενων αναγκών διαλειτουργικότητας.

3. **Ασφάλεια και συμμόρφωση με GDPR**

- Χρήση SSL/TLS για ασφαλή επικοινωνία
- Κρυπτογράφηση δεδομένων εντός της βάσης και κατά τη μεταφορά.
- Συμμόρφωση με τις απαιτήσεις του Κανονισμού προστασίας προσωπικών δεδομένων (GDPR).
- Πρόβλεψη για διατήρηση και λογική διαγραφή δεδομένων σύμφωνα με νομικές απαιτήσεις.
- Πλήρης τήρηση των προδιαγραφών ασφάλειας των συστημάτων δικτύου και πληροφοριών, έτσι όπως αυτές παρατίθενται στο παράρτημα του παρόντος εγγράφου.

4. **Ανθεκτικότητα και Διαθεσιμότητα**

- Λήψη αντιγράφων ασφαλείας (backup) για αποκατάσταση δεδομένων σε περίπτωση απώλειας.
- Monitoring και logging για την ανίχνευση και αντιμετώπιση σφαλμάτων σε πραγματικό χρόνο.

## Γ) Προδιαγραφές ασφάλειας των συστημάτων δικτύου και πληροφορικής

**1.** <u>Καταγραφή Υλικού και Λογισμικού</u>

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

**2.** <u>Ασφαλής Παραμετροποίηση Εξοπλισμού και Εφαρμογών</u>

Ο ανάδοχος θα πρέπει

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

i. 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.

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

iii. 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.

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

v. να υλοποιεί τις παρακάτω ρυθμίσεις στις δικτυακές συσκευές:

i. Απενεργοποίηση κάθε περιττής υπηρεσίας (service).

ii. Στα switches ενεργοποίηση της λειτουργίας "port security".

iii. Στους δρομολογητές (routers) απενεργοποίηση των interfaces και των πρωτόκολλων δρομολόγησης που δεν χρησιμοποιούνται.

iv. Στα switches απενεργοποίηση των θυρών που δεν χρησιμοποιούνται.

v. Εφαρμογή αυθεντικοποίησης δύο παραγόντων (2-factor authentication) για την πρόσβαση στο διαχειριστικό περιβάλλον όλων των κρίσιμων δικτυακών συσκευών.

vi. 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.

vii. Διασφάλιση ότι τα προεπιλεγμένα συνθηματικά (default passwords) σε κάθε νέο προϊόν τροποποιούνται κατά την πρώτη εγκατάσταση του προϊόντος.

viii. 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).

**Δ) Έλεγχος Εκτέλεσης Προγραμμάτων και Υπηρεσιών**

Ο ανάδοχος θα πρέπει:

vi. έχει αναπτύξει καταγεγραμμένη πολιτική, καθώς και διαδικασίες υλοποίησης, που αφορούν στον έλεγχο εγκατάστασης και εκτέλεσης προγραμμάτων και υπηρεσιών στο δίκτυο και στα συστήματά του.

vii. 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.

viii. 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.

ix. 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).

x. 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.

xi. 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.

xii. διασφαλίσει ότι οι χρήστες με standard δικαιώματα (non-privileged) δεν μπορούν να απενεργοποιήσουν ή να τροποποιήσουν τις ρυθμίσεις ασφάλειας στο λειτουργικό τους σύστημα.

xiii. 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).

xiv. 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).

xv. έχει απενεργοποιήσει τις εκδόσεις SMBv1 και v2 στο εσωτερικό δίκτυο και να έχει αναβαθμίσει στην έκδοση v3 ή στην πλέον πρόσφατη.

**3.** <u>Διαχείριση Λογαριασμών και Έλεγχος Πρόσβασης</u>

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).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.

ix. 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.).

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

xi. 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.

**4.** 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.

**5.** 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.

**6.** <u>Τήρηση και ανάλυση αρχείων καταγραφής συμβάντων (event logs)</u>

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 (logout) για όλα τα συστήματα που απαιτούν αυθεντικοποίηση.

iv. έχει ενεργοποιήσει την καταγραφή όλων των δραστηριοτήτων που αφορούν σε διαχειριστικούς λογαριασμούς.

v. 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.

vi. έχει ρυθμίσει τα αρχεία καταγραφής συμβάντων να περιλαμβάνουν λεπτομερή metadata όπως πηγή γεγονότος, ημερομηνία, χρήστης, χρονοσήμανση, IP διεύθυνση πηγής, IP διεύθυνση προορισμού κ.λπ.

vii. έχει διασφαλίσει ότι τα αρχεία καταγραφής συμβάντων τηρούνται για χρονική περίοδο κατ' ελάχιστον ενός (1) έτους.

viii. έχει διασφαλίσει ότι τα αρχεία καταγραφής συμβάντων προστατεύονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση και διαγραφή.

ix. έχει διασφαλίσει ότι η διαχείριση της λειτουργίας καταγραφής συμβάντων έχει ανατεθεί σε ένα υποσύνολο χρηστών με λογαριασμούς αυξημένων προνομίων.

**7.** 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.

**8.** 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 δραστηριότητας. Χρήση Κρυπτογράφησης

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.

**9.** <u>Υλοποίηση Τεχνικών Κυβερνοασφάλειας</u>

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 κυβερνο-εγκληματιών.
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.

**10.** 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.

# ΠΑΡΑΡΤΗΜΑ 3
## Κατάρτιση Προσφοράς

**3.1. Προϋποθέσεις συμμετοχής**

Προσφορά που αποκλίνει από τις ανωτέρω τεχνικές προδιαγραφές και προϋποθέσεις θα κριθεί ως απαράδεκτη και θα απορριφθεί.

**3.2. Δικαιολογητικά Συμμετοχής**

Τα στοιχεία και δικαιολογητικά για την συμμετοχή του προσκαλούμενου οικονομικού φορέα στη διαγωνιστική διαδικασία περιλαμβάνουν με 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 έκδοσής 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 από το νόμιμο εκπρόσωπο της εταιρίας 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 εταιρίας, στην οποία θα δηλώνεται ότι αποδέχεται πλήρως και ανεπιφύλακτα όλους τους όρους της παρούσας πρόσκλησης.
8. Υπεύθυνη δήλωση υπογεγραμμένη από το νόμιμο εκπρόσωπο της εταιρίας 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».

Σε περίπτωση νομικού προσώπου οι προαναφερόμενες υπεύθυνες δηλώσεις υποβάλλονται εκ μέρους του νόμιμου εκπροσώπου του, όπως αυτός ορίζεται στην περίπτωση 79Α του ν.4412/2016 και αφορά ιδίως: α) στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.), ιδιωτικών κεφαλαιουχικών εταιρειών (Ι.Κ.Ε.) και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.), τους διαχειριστές, β) στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.), τον Διευθύνοντα Σύμβουλο, καθώς και όλα τα μέλη του Διοικητικού Συμβουλίου.(άρθρο 80 παρ. 9 του ν.4412/2016, όπως συμπληρώθηκε με την παρ. 7αγ του άρθρου 43 του ν.4605/2019).

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 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 προσφορά θα κατατεθεί σε κλειστό σφραγισμένο φάκελο, στον οποίο θα πρέπει να βρίσκονται η οικονομική και η τεχνική προσφορά σε ευρώ, καθώς και όλα τα ανωτέρω σχετικά στοιχεία και δικαιολογητικά συμμετοχής. Στην τιμή περιλαμβάνονται οι υπέρ τρίτων κρατήσεις και κάθε άλλη επιβάρυνση, σύμφωνα με την κείμενη νομοθεσία.

Οι υπέρ τρίτων κρατήσεις υπόκεινται στο εκάστοτε ισχύον αναλογικό τέλος χαρτοσήμου και στην επ’ αυτού εισφορά υπέρ ΟΓΑ.

Η προσφερόμενη τιμή είναι σταθερή καθ’ όλη τη διάρκεια της σύμβασης και δεν αναπροσαρμόζεται.

Ως απαράδεκτη θα απορριφθεί η προσφορά εφόσον:

α) δεν 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 ΦΠΑ υπερβαίνει τον συνολικό προϋπολογισμό άνευ ΦΠΑ της παρούσας πρόσκλησης.

Η τεχνική προσφορά πρέπει να καλύπτει όλες τις απαιτήσεις και τις προδιαγραφές της παρούσας πρόσκλησης και των Παραρτημάτων αυτής. Περιλαμβάνει ιδίως τα έγγραφα και δικαιολογητικά, βάσει των οποίων θα αξιολογηθεί η καταλληλότητα των προσφερόμενων αγαθών.

**3.4 Χρόνος ισχύος της προσφοράς**

Η προσφορά ισχύει και δεσμεύει τον ενδιαφερόμενο οικονομικό φορέα για τριάντα (30) ημέρες 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. 1 α του ν. 4412/2016, κατ' ανώτατο όριο για χρονικό διάστημα ίσο με την προβλεπόμενη ως άνω αρχική διάρκεια.

## <u>ΠΑΡΑΡΤΗΜΑ 4</u>

### Οικονομικά Στοιχεία του Έργου

Φορέας χρηματοδότησης της παρούσας σύμβασης είναι το Υπουργείο Εσωτερικών. Η παρούσα σύμβαση βαρύνει τις πιστώσεις του Προϋπολογισμού Δημοσίων Επενδύσεων (ΠΔΕ) και συγκεκριμένα του Κωδικού **ΣΑ ΝΑ655** με κωδικό εναρίθμου **2024ΝΑ65500000,** με την εκτιμώμενη αξία της σύμβασης να ανέρχεται στο ποσό των εξήντα χιλιάδων ευρώ (**60.000,00 €)** μη συμπεριλαμβανομένου Φ.Π.Α. 24 %, ήτοι στο ποσό των

εβδομήντα τεσσάρων χιλιάδων τετρακοσίων ευρώ (**74.400,00 €**), για τη δημιουργία νέου Πληροφοριακού Συστήματος (ΠΣ) Διαχείρισης Πληρωμών Προγραμμάτων του Υπουργείου Εσωτερικών.

## ΠΑΡΑΡΤΗΜΑ 5
### Εγγυητική επιστολή καλής εκτέλεσης

Για την υπογραφή της σύμβασης απαιτείται η παροχή εγγύησης καλής εκτέλεσης, σύμφωνα με το άρθρο 72 παρ. 4 του ν. 4412/2016, το ύψος της οποίας ανέρχεται σε ποσοστό **4%** επί της εκτιμώμενης αξίας της σύμβασης, ή του τμήματος αυτής, ήτοι στο ποσό των **δύο χιλιάδων τετρακοσίων ευρώ** (**2.400,00€)** και η οποία κατατίθεται μέχρι και την υπογραφή του συμφωνητικού.

Η εγγύηση καλής εκτέλεσης, προκειμένου να γίνει αποδεκτή, πρέπει να περιλαμβάνει κατ' ελάχιστον τα αναφερόμενα στην παρ. 12 του άρθρου 72 του ν. 4412/2016 στοιχεία και, επιπλέον, τον τίτλο και τον αριθμό της σχετικής σύμβασης, εφόσον ο τελευταίος είναι γνωστός. Το περιεχόμενό της είναι σύμφωνο με τα οριζόμενα στο άρθρο 72 του ν. 4412/2016.

Η εγγύηση καλής εκτέλεσης της σύμβασης καλύπτει συνολικά και χωρίς διακρίσεις την εφαρμογή όλων των όρων της σύμβασης και κάθε απαίτηση της αναθέτουσας αρχής έναντι του αναδόχου.

Η εγγύηση καλής εκτέλεσης καταπίπτει υπέρ της αναθέτουσας αρχής στην περίπτωση παραβίασης, από τον ανάδοχο, των όρων της σύμβασης, όπως αυτή ειδικότερα ορίζει.

Η εγγύηση καλής εκτέλεσης επιστρέφεται στο σύνολό της μετά από την ποσοτική και ποιοτική παραλαβή του συνόλου του αντικειμένου της σύμβασης.

Σε περίπτωση που στο πρωτόκολλο οριστικής και ποσοτικής παραλαβής αναφέρονται παρατηρήσεις ή υπάρχει εκπρόθεσμη παράδοση, η επιστροφή της εγγύησης καλής εκτέλεσης γίνεται μετά από την αντιμετώπιση, σύμφωνα με όσα προβλέπονται, των παρατηρήσεων και του εκπρόθεσμου.

## ΠΑΡΑΡΤΗΜΑ 6
### Χρονική διάρκεια σύμβασης

Η διάρκεια της σύμβασης ορίζεται και εκτείνεται για τέσσερις (4) μήνες από την υπογραφή της.

## ΠΑΡΑΡΤΗΜΑ 7

### 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 Ι) 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.