@ΣΗΔΕ ΙΡΙΔΑ
67bdce2b877b1a1eecc15017
ΑΠ:12170
Υπογραφή: 06/03/25 16:49
Διανομή: 07/03/25 13:02

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ
ΓΕΝ. Δ/ΝΣΗ ΟΙΚΟΝΟΜΙΚΩΝ ΥΠΗΡΕΣΙΩΝ
& ΔΙΟΙΚΗΤΙΚΗΣ ΥΠΟΣΤΗΡΙΞΗΣ
ΔΙΕΥΘΥΝΣΗ ΠΡΟΜΗΘΕΙΩΝ & ΥΠΟΔΟΜΩΝ
ΤΜΗΜΑ ΠΡΟΜΗΘΕΙΩΝ
Πληροφορίες : Ι. Χρυσούλης
E-mail : i.chrysoulis@ypes.gr
Τηλέφωνο : 2131361671
Ταχ. Δ/νση : Σταδίου 31
Ταχ. Κώδικας : 10183

Αθήνα, 06-03-2025
Αρ. πρωτ.: 12170

ΠΡΟΣ: MODUS A.E.
sales@modus.gr

ΘΕΜΑ: Πρόσκληση για την κατάθεση οικονομικής προσφοράς για την παροχή υπηρεσιών συντήρησης των Πληροφοριακών Συστημάτων Εξετάσεων απόκτησης του ΠΕΓΠ.

Έχοντας υπόψη :
1) Το αρ. 32 § 2 του ν.4412/2016.
2) τη με αριθμό 1668/2021 (ΑΔΑΜ: 21SYMV008165661) σύμβαση μεταξύ της «Κοινωνίας της Πληροφορίας Α.Ε.» και της «MODUS A.E.» για την «Παροχή υπηρεσιών ανάπτυξης Ολοκληρωμένου Πληροφοριακού Συστήματος Εξετάσεων κτήσης του Πιστοποιητικού Επάρκειας Γνώσεων για Πολιτογράφηση»
3) τη με αριθμό 1783/2021 (ΑΔΑΜ: 21SYMV009239851) σύμβαση μεταξύ της «Κοινωνίας της Πληροφορίας Α.Ε.» και της «MODUS A.E.» για την «Ανάπτυξη συστήματος επιλογής Αξιολογητών/Επιτηρητών, καταγραφής βαθμολογιών και αποτελεσμάτων για τις εξετάσεις κτήσης του Πιστοποιητικού Επάρκειας Γνώσεων της ΓΓΙ» »,
4) τη με αριθμό 27/2022 (ΑΔΑΜ: 22SYMV011470971) σύμβαση μεταξύ του Υπουργείου Εσωτερικών και της «MODUS A.E.» για την «Συντήρηση του Πληροφοριακού Συστήματος Εξετάσεων Πολιτογράφησης Αλλοδαπών, που περιλαμβάνει: 1. το Ολοκληρωμένο Πληροφοριακό Σύστημα Εξετάσεων κτήσης Π.ΕΓ.Π. και 2. το Σύστημα επιλογής Αξιολογητών/Επιτηρητών, καταγραφής βαθμολογιών και αποτελεσμάτων για τις εξετάσεις κτήσης Π.ΕΓ.Π της Γενικής Γραμματείας Ιθαγένειας', για χρονικό διάστημα, από την υπογραφή της σύμβασης έως την 31-12-2024»,
5) την από 13-02-2025 Βεβαίωση Κατασκευαστή της «MODUS A.E.» για την κυριότητα της εταιρίας επί του σχετικού λογισμικού και την δυνατότητα πραγματοποίησης αναγκαίων αλλαγών ή/και τροποποιήσεων που διαθέτει ίδια,
6) την ανάγκη παροχής υπηρεσιών συντήρησης των Πληροφοριακών Συστημάτων Εξετάσεων απόκτησης του ΠΕΓΠ ,
7) το γεγονός ότι ως γνωμοδοτικό όργανο, βάσει του άρθρου 32α §2 του ν. 4412/2016, ορίζεται, η αρμόδια για την παραλαβή «[…] πληροφοριακών συστημάτων και παντός είδους συναφών υλικών και εργασιών συντήρησης και επισκευής αυτών, […]» Επιτροπή Παραλαβής, βάσει της αρ. 32836/04-04-2024 (ΑΔΑ: 621Β46ΜΤΛ6-6ΦΧ) Απόφασης του Υπηρεσιακού Γραμματέα του Υπουργείου Εσωτερικών,

το Υπουργείο Εσωτερικών προσκαλεί, **μέσω διαδικασίας διαπραγμάτευσης χωρίς προηγούμενη δημοσίευση**, την εταιρία με την επωνυμία «MODUS ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ ΥΨΗΛΗΣ ΤΕΧΝΟΛΟΓΙΑΣ, ΕΦΑΡΜΟΓΩΝ ΚΑΙ ΜΕΘΟΔΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ» και δ.τ. «MODUS A.E.»), όπως καταθέσει την οικονομική της προσφορά για την παροχή συντήρησης των Πληροφοριακών Συστημάτων Εξετάσεων απόκτησης του ΠΕΓΠ για χρονικό διάστημα από την υπογραφή της σχετικής σύμβασης και για ένα (1) έτος, με δυνατότητα επέκτασης έως τις 31-12-2026. Η προσφυγή στην διαδικασία της διαπραγμάτευσης χωρίς προηγούμενη δημοσίευση γίνεται καθώς ο προσκαλούμενος

οικονομικός φορέας διαθέτει μοναδική ικανότητα παροχής των ζητούμενων υπηρεσιών για τεχνικούς λόγους αλλά και δικαιώματα πνευματικής ιδιοκτησίας επί του πηγαίου κώδικα του υπό συντήρηση λογισμικού και συνεπώς συντρέχουν οι προϋποθέσεις των υποπεριπτώσεων ββ' και γγ΄ της περίπτωσης β' της παραγράφου 2 του αρ. 32 του ν.4412/2016, αντίστοιχα. Η εν λόγω οικονομική προσφορά θα διαμορφωθεί 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 Ζητούμενων Υπηρεσιών
- Παράρτημα 3: Κατάρτιση Προσφοράς.
- Παράρτημα 4: Υποχρέωση εχεμύθειας και εμπιστευτικότητας – Προστασία προσωπικών δεδομένων.

Ο ΥΠΗΡΕΣΙΑΚΟΣ ΓΡΑΜΜΑΤΕΑΣ

ΠΑΝΤΕΛΗΣ ΤΑΓΚΑΛΑΚΗΣ

<u>Εσωτερική Διανομή:</u>

1. Γραφείο Γενικού Γραμματέα Ιθαγένειας
2. Γραφείο Υπηρεσιακού Γραμματέα
3. Γενική Διεύθυνση Ιθαγένειας
4. Διεύθυνση Προμηθειών και 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	Η ανάθεση θα γίνει βάσει 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 της περ. β' παρ. 2 του άρθρου 32 και του άρθρου $32^{Α}$ (διαδικασία διαπραγμάτευσης χωρίς προηγούμενη δημοσίευση).
ΑΝΑΛΥΣΗ ΘΕΜΑΤΟΣ	Το Υπουργείο Εσωτερικών προτίθεται να προβεί στην ανάθεση παροχής υπηρεσιών συντήρησης των Πληροφοριακών Συστημάτων Εξετάσεων απόκτησης του ΠΕΓΠ. Οι προδιαγραφές της εν λόγω παροχής αναφέρονται στα Παραρτήματα 1, 2, 3 και 4 τα οποία αποτελούν αναπόσπαστο μέρος της παρούσας **(ΕΠΙ ΠΟΙΝΗ ΑΠΟΚΛΕΙΣΜΟΥ).**
ΠΡΟΣΚΑΛΟΥΜΕΝΟΙ ΦΟΡΕΙΣ	**Η πρόσκληση απευθύνεται αποκλειστικά στην εταιρεία «MODUS ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ ΥΨΗΛΗΣ ΤΕΧΝΟΛΟΓΙΑΣ, ΕΦΑΡΜΟΓΩΝ ΚΑΙ ΜΕΘΟΔΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ»** Δεν λαμβάνονται υπόψη προσφορές οικονομικών φορέων που δεν προσκλήθηκαν να υποβάλλουν προσφορά.
ΕΚΤΙΜΩΜΕΝΟ ΚΟΣΤΟΣ ΓΙΑ ΤΗΝ ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ ΓΙΑ ΕΝΑ (1) ΕΤΟΣ	Ποσό άνευ Φ.Π.Α.: : Έως 65.000,00**€** Ποσό συμπεριλαμβανομένου Φ.Π.Α 24% : 80.600,00**€**
ΕΚΤΙΜΩΜΕΝΟ ΣΥΝΟΛΙΚΟ ΚΟΣΤΟΣ ΓΙΑ ΤΗΝ ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ ΕΩΣ ΤΙΣ 31-12-2026	Ποσό άνευ Φ.Π.Α.: : Έως 119.166,67**€** Ποσό συμπεριλαμβανομένου Φ.Π.Α 24% : 147.766,65 **€**
ΝΟΜΙΣΜΑ	Ευρώ
ΤΕΚΜΗΡΙΩΜΕΝΟ ΑΙΤΗΜΑ ΑΝΑΛΗΨΗΣ ΥΠΟΧΡΕΩΣΗΣ : ΑΠΟΦΑΣΗ ΑΝΑΛΗΨΗΣ ΥΠΟΧΡΕΩΣΗΣ ΓΙΑ ΤΟ 2025: ΑΠΟΦΑΣΗ ΑΝΑΛΗΨΗΣ ΠΟΛΥΕΤΟΥΣ ΥΠΟΧΡΕΩΣΗΣ:	Αρ. πρωτ. 3862/23-1-2025 (ΑΔΑΜ: 25REQ016203278) Αρ. πρωτ. 8267/13-02-2025 (ΑΔΑ: 9ΞΝΣ46ΜΤΛ6-Ξ0Ο, ΑΔΑΜ: 25REQ016353777) Αρ. πρωτ. 7311/10-02-2025 (ΑΔΑ: ΨΘΖΡ46ΜΤΛ6-8ΤΟ, ΑΔΑΜ: 25REQ016353794)

ΚΩΔΙΚΟΣ ΠΡΟΫΠΟΛΟΓΙΣΜΟΥ ΦΟΡΕΑ	Τακτικός Προϋπολογισμός, Ειδικός Φορέας 1007-202 **ΑΛΕ 2420389001**
CPV	72267000-4 Υπηρεσίες συντήρησης και επισκευής λογισμικού.
ΠΑΡΑΚΡΑΤΗΣΗ ΦΟΡΟΥ ΕΠΙ ΤΗΣ ΚΑΘΑΡΗΣ ΣΥΜΒΑΤΙΚΗΣ ΑΞΙΑΣ	**Φόρος**: 8% 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).
ΔΙΑΡΚΕΙΑ ΣΥΜΒΑΣΗΣ	Από την υπογραφή της σύμβασης και για ένα (1) έτος, με δυνατότητα επέκτασης έως τις 31-12-2026.
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 στο ν. 4601/2019 και στις ΚΥΑ με αριθμό 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 με αριθμό Α.1035/18.02.2020 (Β΄551) και Α.1138/12.06.2020 (Β΄2470), στις οποίες μεταξύ άλλων προβλέπεται η χρήση παροχών υπηρεσιών ηλεκτρονικής έκδοσης στοιχείων. Περισσότερες πληροφορίες μπορείτε να βρείτε στο σύνδεσμο https://www.gsis.gr/polites-epiheiriseis/plirromes-kai-eispraxeis/e-invoice
ΚΩΔΙΚΟΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΙΜΟΛΟΓΗΣΗΣ ΦΟΡΕΑ (ΑΑΗΤ):	1007.0000000000.0001
ΚΑΤΑΛΗΚΤΙΚΗ ΠΡΟΘΕΣΜΙΑ ΚΑΤΑΘΕΣΗΣ ΠΡΟΣΦΟΡΩΝ	**Μέχρι την Τρίτη 11 Μαρτίου 2025 και ώρα 12:00΄** Οι προσφορές και τα απαιτούμενα δικαιολογητικά θα υποβληθούν **σε κλειστό φάκελο**.
ΤΟΠΟΣ ΚΑΤΑΘΕΣΗΣ ΠΡΟΣΦΟΡΩΝ	Υπουργείο Εσωτερικών Δ/νση Προμηθειών & Υποδομών Τμήμα Προμηθειών Σταδίου 31, 4ος όροφος, Τ.Κ. 101 83 Αθήνα Τηλέφωνο επικοινωνίας για διευκρινίσεις: Γιάννης Χρυσούλης : 2131361671

	Email: i.chrysoulis@ypes.gr
ΕΝΗΜΕΡΩΣΗ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	Η Αναθέτουσα Αρχή ενημερώνει υπό την ιδιότητά της ως υπεύθυνης επεξεργασίας το φυσικό πρόσωπο που υπογράφει την προσφορά ως Προσφέρων ή ως Νόμιμος Εκπρόσωπος Προσφέροντος, ότι η ίδια ή και τρίτοι, κατ' εντολή και για λογαριασμό της, 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) Φορείς στους οποίους 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. (γ) Έτεροι συμμετέχοντες στο Διαγωνισμό, στο πλαίσιο της αρχής της διαφάνειας και του δικαιώματος προδικαστικής και δικαστικής προστασίας των συμμετεχόντων στο Διαγωνισμό, σύμφωνα με το νόμο. 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. 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.
ΚΑΝΟΝΕΣ ΔΗΜΟΣΙΟΤΗΤΑΣ	Η παρούσα ανακοίνωση να αναρτηθεί: α) στην ιστοσελίδα του ΥΠΕΣ www.ypes.gr, β) στο Κεντρικό Ηλεκτρονικό Μητρώο Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ) www.eprocurement.gov.gr

ΠΑΡΑΡΤΗΜΑ 2

Τεχνικές Προδιαγραφές Ζητούμενων Υπηρεσιών

2.1 Αναλυτικές Τεχνικές Προδιαγραφές

Ο υποψήφιος ανάδοχος θα παρέχει υπηρεσίες συντήρησης και τεχνικής υποστήριξης των πληροφοριακών συστημάτων, τα οποία υποστηρίζουν την διενέργεια των Εξετάσεων Πιστοποιητικού Επάρκειας Γνώσεων για Πολιτογράφηση (Π.Ε.Γ.Π) και είναι τα ακόλουθα:

- Ολοκληρωμένο Πληροφοριακό Σύστημα Εξετάσεων κτήσης του Πιστοποιητικού Επάρκειας Γνώσεων για Πολιτογράφηση.
- Σύστημα επιλογής Αξιολογητών / Επιτηρητών, καταγραφής βαθμολογιών και αποτελεσμάτων για τις εξετάσεις κτήσης του Πιστοποιητικού Επάρκειας Γνώσεων.
- Enterprise Content Management System Papyros Release 7.5 – Το οποίο αποτελεί την πλατφόρμα λογισμικού στο οποίο υλοποιήθηκαν τα δύο παραπάνω πληροφοριακά συστήματα.

Ανά εξεταστική περίοδο απαιτούνται υπηρεσίες τεχνικής υποστήριξης των συστημάτων πληροφορικής καθώς και αλλαγές λειτουργικότητας (εξελικτική συντήρηση), σύμφωνα με τις εκάστοτε ανάγκες.
Για την εύρυθμη λειτουργία του ΠΣ Εξετάσεων Απόκτησης Ιθαγένειας, απαιτούνται σε τακτική βάση:

- υπηρεσίες τεχνικής υποστήριξης κατά την διάρκεια του κάθε εξαμηνιαίου κύκλου εξετάσεων,
- συντήρησης λογισμικού (α) διορθώσεις δυσλειτουργιών (επανορθωτική συντήρηση) και β) αλλαγές και προσθήκες λειτουργικότητας σύμφωνα με νέες ανάγκες (εξελικτική συντήρηση)
- Software Assurance του λογισμικού Papyros, στο οποίο υλοποιήθηκε το εν λόγω ΠΣ

Για κάθε νέα εξεταστική Περίοδο αναλυτικά χρειάζονται να γίνονται οι παρακάτω εργασίες τεχνικής υποστήριξης.

2.1.1. Αιτήσεις Υποψηφίων

Αρχικοποίηση νέας περιόδου

- Ενημέρωση της Τράπεζας Θεμάτων για την νέα εξεταστική περίοδο
    - Επιλογή θεμάτων της προηγούμενης περιόδου και αναπαραγωγή τους στην νέα
    - Προσθήκη νέων θεμάτων που αντικαθιστούν τα προηγούμενα
    - Δημιουργία αρχείων απαντήσεων με βάση τις αλλαγές στην τράπεζα
- Εισαγωγή των πόλεων που θα λειτουργούν εξεταστικά κέντρα στην νέα εξεταστική
- Ενημέρωση των υποψηφίων που δεν έλαβαν μέρος στην προηγούμενη εξεταστική περίοδο και είχαν δικαιολογημένη απουσία
- Ενημέρωση των ήδη πληρωμένων παράβολων των υποψηφίων που δεν έλαβαν μέρος στην προηγούμενη εξεταστική περίοδο και είχαν δικαιολογημένη απουσία
- Καταχώριση ανακοινώσεων της Γενικής Γραμματείας σε σχέση με την έναρξη της εξεταστικής περιόδου

Περίοδος υποβολής αιτήσεων

- Υποστήριξη χρηστών για απορίες / δυσλειτουργίες στην πλατφόρμα υποβολής αιτήσεων
- Παραγωγή στατιστικών σε σχέση με τους υποψηφίους
- Μαζικές αποστολές email για ενημέρωση των υποψηφίων σε θέματα που αφορούν τις εξετάσεις

Ολοκλήρωση υποβολής αιτήσεων

- Αλλαγές στα εξεταστικά κέντρα με προσθήκη νέων / συγχώνευση υπαρχόντων
- Μαζικές αποστολές email για ενημέρωση των αλλαγών των εξεταστικών κέντρων
- Μαζικές αλλαγές επιλογής εξεταστικού κέντρου για τα κέντρα που καταργούνται
- Προτάσεις επιλογής εξεταστικού κέντρου σε υποψηφίους με βάση τα γεωγραφικά τους στοιχεία για τα νέα κέντρα
- Παραγωγή στατιστικών στοιχείων σε σχέση με τους υποψηφίους
- Αρχικοποίηση των σχολείων στις πόλεις που θα λειτουργήσουν τα εξεταστικά κέντρα
- Κατανομή των υποψηφίων στα σχολεία με βάση στοιχεία γεωγραφικής κατανομής και με βάση μεταβλητούς κανόνες π.χ. Δήμος / Π.Ε., σειρά που έχει υποβάλει την αίτηση κλπ
- Μαζικές αποστολές email για ενημέρωση σε σχέση με το εξεταστικό κέντρο που θα πάρουν μέρος οι υποψήφιοι
- Μαζική παραγωγή των δελτίων εξεταζόμενων
- Μαζικές αποστολές email προς τους υποψήφιους για ενημέρωση
- Αλλαγές στοιχείων σε σχέση με τις εξετάσεις

Εξετάσεις

- Δημιουργία καταστάσεων συμμετεχόντων στις εξετάσεις
- Υποστήριξη της διαδικασίας των εξετάσεων
- Παραλαβή παρουσιών από εξεταστικά κέντρα και εισαγωγή τους στην πλατφόρμα
- Εξαγωγή στατιστικών για τις παρουσίες στις εξετάσεις
- Ενημερώσεις για δικαιολογημένες απουσίες
- Μαζική αποστολή email ώστε να δηλωθούν τα δικαιολογητικά των δικαιολογημένα απόντων
-

Βαθμολογίες

- Παραλαβή των αποτελεσμάτων και εισαγωγή τους στην πλατφόρμα
- Υπολογισμός των αποτελεσμάτων
- Εξαγωγή στατιστικών αποτελεσμάτων

2.1.2.Αιτήσεις Βαθμολογητών

Αρχικοποίηση νέας περιόδου

- Αρχικοποίηση των χαρακτηριστικών των προσόντων των βαθμολογητών
- Αρχικοποίηση των εξεταστικών κέντρων που θα δηλώσουν οι βαθμολογητές /Αξιολογητές
- Αρχικοποίηση των κανόνων σε σχέση με το πλήθος και τον τύπο των επιλογών που μπορεί να κάνει ο κάθε βαθμολογητής / αξιολογητής

Περίοδος υποβολής αιτήσεων

- Υποστήριξη χρηστών για απορίες / δυσλειτουργίες στην πλατφόρμα υποβολής αιτήσεων
- Παραγωγή στατιστικών
- Μαζικές αποστολές email για ενημέρωση σε θέματα που αφορούν τα εξεταστικά κέντρα

Εξετάσεις

- Δημιουργία καταστάσεων συμμετεχόντων στις εξετάσεις
- Υποστήριξη της διαδικασίας των εξετάσεων
- Παραλαβή παρουσιών βαθμολογητών / αξιολογητών που πήραν μέρος στις εξετάσεις

Υποβολή βεβαιώσεων συμμετοχής

- Υποστήριξη χρηστών για απορίες / δυσλειτουργίες στην πλατφόρμα υποβολής βεβαιώσεων

Εκκαθάριση πληρωμών

- Εξαγωγή στατιστικών
- Δημιουργία XML αρχείων πληρωμών σε όλη την διάρκεια εκκαθάρισης
- Ενημέρωση των αιτήσεων με τα ποσά εκκαθάρισης

Αλλαγές στις εφαρμογές

Σε κάθε εξεταστική περίοδο υλοποιούνται αλλαγές στην εφαρμογή που έχουν να κάνουν είτε με στοιχεία που παρατηρήθηκαν και πρέπει να βελτιωθούν είτε με μικρές αλλαγές που προκύπτουν από τις νέες αποφάσεις του Γενικού Γραμματέα Ιθαγένειας. Τέτοιες αλλαγές έχουν να κάνουν με στοιχεία όπως τα παρακάτω:

- Αναγκαία στοιχεία για την υποβολή της αίτησης μπορούν να προστεθούν ή να αφαιρεθούν και να αλλάξει αν είναι υποχρεωτικά
- Αλλαγή του αριθμού των εξεταστικών κέντρων που μπορούν να δηλώσουν οι υποψήφιοι καθώς και του αλγορίθμου επιτρεπτών επιλογών
- Αλλαγές στην φόρμα υποβολής αιτήσεων βαθμολογητών / αξιολογητών
- Προσθήκη νέων ελέγχων μέσω διαλειτουργικότητας με τρίτα συστήματα π.χ. έλεγχος ΑΦΜ-ΑΜΚΑ

Επίσης, το πλαίσιο Υπηρεσιών Τεχνικής Υποστήριξης θα πρέπει να περιλαμβάνει τα παρακάτω:

- Συντήρηση του λογισμικού με (α) διορθώσεις δυσλειτουργιών (επανορθωτική συντήρηση) και β) αλλαγές και προσθήκες λειτουργικότητας σύμφωνα με νέες ανάγκες (εξελικτική συντήρηση)
- Παράδοση και εγκατάσταση των νέων εκδόσεων του λογισμικού ECM (releases & new versions).
- Τηλεφωνική υποστήριξη και πρόσβαση στο Κέντρο Αναφοράς Βλαβών (Help–Desk). Το Help Desk του αναδόχου θα πρέπει να είναι διαθέσιμο καθ’ όλη την περίοδο συντήρησης και κατά τις εργάσιμες ημέρες και ώρες, καταγράφοντας τα αιτήματα των χρηστών, δρομολογώντας τα στα κατάλληλα τμήματα της εταιρίας μας για την επίλυση των προβλημάτων και υποστηρίζοντας τηλεφωνικά και μέσω διαδικτύου τους χρήστες και διαχειριστές του πληροφοριακού συστήματος.

2.2 Προδιαγραφές Ασφαλείας

2.2.1 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

2.2.2 Ασφαλής Παραμετροποίηση Εξοπλισμού και Εφαρμογών

Ο ανάδοχος θα πρέπει

- να **παραδώσει** πολιτική και διαδικασίες ασφαλούς παραμετροποίησης εξοπλισμού, λειτουργικών συστημάτων και εφαρμογών
- 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.
- να χρησιμοποιεί μόνο υποστηριζόμενες εκδόσεις για τα λειτουργικά συστήματα των σταθμών εργασίας, των servers και των δικτυακών συσκευών.
- 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.
- να χρησιμοποιεί μόνο τις τελευταίες και ενημερωμένες εκδόσεις για κάθε server εφαρμογή του που είναι προσβάσιμη από το Internet.
- 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).

2.2.3 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.

2.2.4 Διαχείριση Λογαριασμών και Έλεγχος Πρόσβασης

Ο ανάδοχος θα πρέπει να

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

- έχει υλοποιήσει μηχανισμό για να απενεργοποιεί λογαριασμούς χρηστών ύστερα από συγκεκριμένο χρονικό διάστημα αδρανούς δραστηριότητας (π.χ. 3 μήνες).
- 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).
- 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.
- 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.).
- έχει υλοποιήσει κεντρική διαχείριση λογαριασμών μέσω υπηρεσίας καταλόγου (π.χ.
- Active directory service).
- 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.

2.2.5 Αυθεντικοποίηση Χρηστών

Ο ανάδοχος θα πρέπει

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

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

2.2.6 Ασφάλεια Δικτύων.

Ο ανάδοχος θα πρέπει

- να τηρεί επικαιροποιημένο διάγραμμα δικτύου και ροής δεδομένων (network and data flow diagram), στο οποίο απεικονίζονται όλες οι δικτυακές συνδέσεις
- να τηρεί σε προστατευμένο αρχείο όλους τους κανόνες δρομολόγησης, καθώς και τους κανόνες ελέγχου πρόσβασης (access control lists) των firewalls.
- 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).
- 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.
- 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.
- 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.
- να υλοποιεί firewall επιπέδου εφαρμογής (application firewall) μπροστά από κάθε κρίσιμης σημασίας server, με σκοπό τον αποκλεισμό της κακόβουλης κίνησης.
- να υλοποιήσει δικτυακά συστήματα ανίχνευσης και πρόληψης εισβολών (network intrusion detection / prevention systems), με σκοπό την ανίχνευση και πρόληψη επιθέσεων.
- να έχει διασφαλίσει ότι η υποδομή του διαθέτει πλεονασμό σε πόρους που της επιτρέπουν να ανθίσταται σε επίθεση άρνησης παροχής υπηρεσιών.
- να έχει διαχωρίσει δικτυακά τις κρίσιμες υπηρεσίες του από άλλες υπηρεσίες που είναι πιθανότερο να στοχοποιηθούν (π.χ. web υπηρεσίες).
- να υλοποιεί συστήματα παρακολούθησης της διαθεσιμότητας των κρίσιμων υπηρεσιών του, που ανιχνεύουν επιθέσεις άρνησης παροχής υπηρεσιών και στέλνουν ειδοποίηση σε πραγματικό χρόνο.
- 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.

2.2.7 Τήρηση και ανάλυση αρχείων καταγραφής συμβάντων (event logs)

Ο ανάδοχος θα πρέπει να

- έχει ενεργοποιήσει τη λειτουργία καταγραφής συμβάντων (event logs) σε όλους τους σταθμούς εργασίας, servers και δικτυακές συσκευές.
- έχει διασφαλίσει τον συγχρονισμό ανάμεσα στα ρολόγια όλων των συσκευών, έτσι ώστε να επιτυγχάνεται ακρίβεια στη συσχέτιση συμβάντων μεταξύ διαφορετικών συστημάτων.
- έχει ενεργοποιήσει την καταγραφή επιτυχούς και ανεπιτυχούς εισόδου (login) και εξόδου (logout) για όλα τα συστήματα που απαιτούν αυθεντικοποίηση.
- έχει ενεργοποιήσει την καταγραφή όλων των δραστηριοτήτων που αφορούν σε διαχειριστικούς λογαριασμούς.
- 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.
- έχει ρυθμίσει τα αρχεία καταγραφής συμβάντων να περιλαμβάνουν λεπτομερή metadata όπως πηγή γεγονότος, ημερομηνία, χρήστης, χρονοσήμανση, IP διεύθυνση πηγής, IP διεύθυνση προορισμού κ.λπ.
- έχει διασφαλίσει ότι τα αρχεία καταγραφής συμβάντων τηρούνται για χρονική περίοδο κατ' ελάχιστον ενός (1) έτους.
- έχει διασφαλίσει ότι τα αρχεία καταγραφής συμβάντων προστατεύονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση, τροποποίηση και διαγραφή.
- έχει διασφαλίσει ότι η διαχείριση της λειτουργίας καταγραφής συμβάντων έχει ανατεθεί σε ένα υποσύνολο χρηστών με λογαριασμούς αυξημένων προνομίων.

2.2.8 Ασφάλεια Διαδικτυακών Εφαρμογών

Ο ανάδοχος θα πρέπει

- 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.
- να διασφαλίζει ότι χρησιμοποιούνται αξιόπιστες και πλήρως ενημερωμένες πλατφόρμες ανάπτυξης εφαρμογών, καθώς και βιβλιοθήκες λογισμικού που προέρχονται από έμπιστες πηγές και συντηρούνται ενεργά.
- 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.
- να διασφαλίζει ότι κατά την ανάπτυξη διαδικτυακών εφαρμογών λαμβάνονται υπόψη κοινοί τύποι ευπαθειών, όπως είναι το OWASP Top-10.
- 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.

- 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).
- 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.
- 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.
- να διασφαλίζει ότι διενεργείται έλεγχος παρείσδυσης (penetration test) πριν η τελική έκδοση της εφαρμογής τεθεί σε παραγωγική λειτουργία.
- 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.
- 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.

2.2.9 Χρήση Κρυπτογραφίας

Ο ανάδοχος θα πρέπει να

- διασφαλίζει ότι τα δεδομένα που έχουν ταξινομηθεί ως κρίσιμα / ευαίσθητα κρυπτογραφούνται κατά τη μετάδοσή τους (encryption in transit).

- 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.
- διασφαλίζει ότι κατά την κρυπτογράφηση χρησιμοποιούνται μόνο τελευταίες εκδόσεις εγκεκριμένων κρυπτογραφικών πρωτοκόλλων και λογισμικού, καθώς επίσης και το κατάλληλο μήκος κλειδιών.
- 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.
- 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.
- να χρησιμοποιεί αυθεντικοποίηση δημοσίου κλειδιού (public key-based authentication) για την υλοποίηση SSH (Secure Shell) συνδέσεων.

2.2.10 Υλοποίηση Τεχνικών Κυβερνοασφάλειας

Ο ανάδοχος θα πρέπει να

- 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.
- υλοποιεί εγκεκριμένη διαδικασία επιδιόρθωσης των ευπαθειών που έχουν ανιχνευθεί στα αγαθά του σε μηνιαία βάση.
- διενεργεί σε περιοδική βάση (π.χ. μία φορά ετησίως) πλήρη αξιολόγηση των ευπαθειών στα πληροφοριακά του συστήματα (vulnerability assessment).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.
- διενεργεί σε περιοδική βάση (π.χ. μία φορά ετησίως) εσωτερικό έλεγχο παρείσδυσης (internal penetration test), με σκοπό την προσομοίωση κυβερνοεπίθεσης στο εσωτερικό δίκτυο.
- 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.
- 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.

2.2.11 Λήψη Αντιγράφων Ασφάλειας

Ο ανάδοχος θα πρέπει να

- 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.
- έχει διασφαλίσει ότι τα ληφθέντα αντίγραφα ασφαλείας προστατεύονται με κρυπτογράφηση κατά τη μεταφορά τους (encryption in transit).
- 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.
- έχει διασφαλίσει ότι τα αντίγραφα ασφαλείας αποθηκεύονται σε τουλάχιστον έναν
- (1) offline προορισμό που δεν είναι συνδεδεμένος σε κάποιο δίκτυο.
- διενεργεί έλεγχο ακεραιότητας των αντιγράφων ασφαλείας σε περιοδική βάση.
- διενεργεί δοκιμή επαναφοράς δεδομένων (restoration) σε περιοδική βάση, με σκοπό την επικύρωση ότι η λήψη αντιγράφων ασφαλείας λειτουργεί με σωστό τρόπο.
- αποθηκεύει τα ληφθέντα αντίγραφα ασφαλείας σε διαφορετικές γεωγραφικά διεσπαρμένες τοποθεσίες.

2.3 Ζητούμενα Δικαιολογητικά Τεχνικής Ικανότητας

Ο προσκαλούμενος οικονομικός φορέας θα πρέπει:

- Να προσκομίσει τα σχετικά ζητούμενα παραδοτέα των ενοτήτων 2.2.1 & 2.2.2.
- Να προσκομίσει υπεύθυνη δήλωση του νόμιμου εκπροσώπου του ότι πληρούνται όλες οι τεχνικές προδιαγραφές και οι προδιαγραφές ασφαλείας του παρόντος Παραρτήματος.
- Να προσκομίσει Πιστοποιητικό ISO 27001 εν ισχύ, συνοδευόμενο από Υπεύθυνη Δήλωση του νόμιμου εκπροσώπου του στην οποία θα βεβαιώνεται ότι τηρούνται όλες οι απαιτήσεις του προτύπου ISO 27001.

2.4 Υποχρέωση ενσωμάτωσης συμπερασμάτων Έκθεσης Εκτίμησης Αντικτύπου(DPIA)

Εν όψει της παραλαβής σχετικής μελέτης εκτίμησης αντίκτυπου για τα προσωπικά δεδομένα (DPIA) για το προς συντήρηση πληροφοριακό σύστημα βάσει της αρ. 67/2024 Συμβασης (ΑΔΑΜ: 24SYMV015853670), ο προσκαλούμενος οικονομικός φορέας υποχρεούται να ενσωματώσει τις παρατηρήσεις της μελέτης, εντός έξι (6) μηνών από την κοινοποίηση τους σε αυτόν.

ΠΑΡΑΡΤΗΜΑ 3

Κατάρτιση Προσφοράς

Δικαιολογητικά

Τα στοιχεία και δικαιολογητικά για την συμμετοχή του προσκαλούμενου οικονομικού φορέα στη διαδικασία περιλαμβάνουν με ποινή αποκλεισμού τα στοιχεία που περιγράφονται ακολούθως:

1. οικονομική προσφορά

2. τεχνική προσφορά σύμφωνα με τους όρους του Παραρτήματος 2

3. υπεύθυνη δήλωση υπογεγραμμένη από τον νόμιμο εκπρόσωπο ότι αποδέχεται πλήρως τους όρους της συγκεκριμένης πρόσκλησης, στους οποίους περιλαμβάνονται και οι όροι των τεχνικών απαιτήσεων και προδιαγραφών των Παραρτημάτων 1-4

4. υπεύθυνη δήλωση στην οποία θα αναφέρεται ότι δεν έχει επιβληθεί σε βάρος του υποψήφιου αναδόχου η οριζόντια ρήτρα αποκλεισμού σύμφωνα με τις διατάξεις του άρθρου 74 του ν.4412/2016, όπως τροποποιήθηκε από το άρθρο 23 του ν. 4782/2021

5. φορολογική ενημερότητα για συμμετοχή σε διαγωνισμούς του Δημοσίου και ασφαλιστική ενημερότητα για κάθε νόμιμη χρήση

τα εν λόγω πιστοποιητικά γίνονται αποδεκτά εφόσον είναι εν ισχύ κατά τον χρόνο υποβολής τους, άλλως, στην περίπτωση που δεν αναφέρεται χρόνος ισχύος, εφόσον έχουν εκδοθεί έως τρεις (3) μήνες πριν την υποβολή τους (άρθρο 80 παρ. 12 του ν.4412/2016, όπως τροποποιήθηκε και ισχύει)

6. απόσπασμα/τα ποινικού μητρώου του διαχειριστή και του Διευθύνοντα Συμβούλου καθώς και των μελών του Δ.Σ., με ημερομηνία έκδοσης έως τρεις (3) μήνες πριν από την υποβολή τους (δύναται να προσκομιστεί υπεύθυνη δήλωση του άρθ. 8 παρ. 4 του ν.1599/1986, εκ μέρους του οικονομικού φορέα ότι δε συντρέχουν οι λόγοι αποκλεισμού της παρ.1 άρθρου 73 του ν.4412/2016, όπως συμπληρώθηκε με την παρ. 7αγ του άρθρου 43 του ν.4506/2019.)

Στην περίπτωση κατάθεσης υπεύθυνης δήλωσης, εντός 10 ημερών από την υπογραφή της σύμβασης θα πρέπει να προσκομιστούν τα ανωτέρω αναφερόμενα αποσπάσματα ποινικού μητρώου.

Καθόσον πρόκειται για νομικά πρόσωπα, οι προαναφερόμενες υπεύθυνες δηλώσεις υποβάλλονται εκ μέρους του νόμιμου εκπροσώπου τους, όπως αυτός ορίζεται στην περίπτωση 79Α του ν.4412/2016 και αφορά ιδίως 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.

7. Υπεύθυνη δήλωση, υπογεγραμμένη από το νόμιμο εκπρόσωπο της εταιρίας, του ν. 1599/1986 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 Σελίδα 18 από 31 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».

Επιπλέον θα πρέπει να προσκομιστούν δικαιολογητικά νόμιμης σύστασης και εκπροσώπησης ως ακολούθως:

Στις περιπτώσεις νομικών προσώπων, προσκομίζονται τα κατά περίπτωση νομιμοποιητικά έγγραφα σύστασης και νόμιμης εκπροσώπησης (όπως καταστατικά, πιστοποιητικά μεταβολών, αντίστοιχα ΦΕΚ, συγκρότηση Δ.Σ. σε σώμα, σε περίπτωση Α.Ε., κλπ., ανάλογα με τη νομική μορφή του προσφέροντα οικονομικού φορέα).

Αναλυτικότερα και καθώς το προσκαλούμενο νομικό πρόσωπο είναι εταιρεία Α.Ε.:

α. Φ.Ε.Κ. σύστασης (για τις Α.Ε. και Ε.Π.Ε., εφόσον υπάρχει)

β. Γενικό Πιστοποιητικό από το Γ.Ε.ΜΗ., με ημερομηνία έκδοσης είτε έως τριών (3) μηνών πριν από την υποβολή του, είτε μεταγενέστερης της κοινοποίησης της παρούσας πρόσκλησης

γ. Πιστοποιητικό Ισχύουσας Εκπροσώπησης από το Γ.Ε.ΜΗ., με ημερομηνία έκδοσης είτε έως τριάντα (30) εργάσιμων ημερών πριν από την υποβολή του, είτε μεταγενέστερης της κοινοποίησης της παρούσας πρόσκλησης

Η ισχύς της προσφοράς πρέπει να είναι τουλάχιστον δύο (2) μήνες από την καταληκτική ημερομηνία υποβολής της προσφοράς και να αναφέρεται στην προσφορά.

Δικαιολογητικά αναδόχου για πληρωμή

Η πληρωμή του αναδόχου θα γίνεται με την ολοκλήρωση των υπηρεσιών του, ετησίως, με χρηματικό ένταλμα πληρωμής, ύστερα από τη βεβαίωση της αρμόδιας επιτροπής παρακολούθησης και παραλαβής των υπηρεσιών για την ορθή εκτέλεση των όρων της Σύμβασης.

Πριν από την πληρωμή ο ανάδοχος οφείλει να προσκομίζει στο Υπουργείο Εσωτερικών το σχετικό ηλεκτρονικό τιμολόγιο

ΠΑΡΑΡΤΗΜΑ 4

Υποχρέωση εχεμύθειας και εμπιστευτικότητας – Προστασία προσωπικών δεδομένων

- 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 στην 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. 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.