|  |
| --- |
| ΣΥΝΟΠΤΙΚΑ ΣΤΟΙΧΕΙΑ ΔΙΑΚΗΡΥΞΗΣ |
| **ΤΙΤΛΟΣ ΣΥΜΒΑΣΗΣ** | Παροχή συμβουλευτικών υπηρεσιών για την ανάπτυξη και εφαρμογή Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) κατά ISO/ IEC 27001:2013, |
| **ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ** | Βουλή των Ελλήνων (ΒτΕ) |
| **ΦΟΡΕΑΣ ΛΕΙΤΟΥΡΓΙΑΣ** | Βουλή των Ελλήνων (ΒτΕ) |
| **ΦΟΡΕΑΣ ΧΡΗΜΑΤΟΔΟΤΗΣΗΣ** | Το Έργο βαρύνει τον Κ.Α 0899 του προϋπολογισμού της Βουλής των Ελλήνων |
| **ΤΟΠΟΣ ΠΑΡΟΧΗΣ**  | Βουλή των Ελλήνων  |
| **ΕΙΔΟΣ ΣΥΜΒΑΣΗΣ** | Υπηρεσία   |
| **ΕΙΔΟΣ ΔΙΑΔΙΚΑΣΙΑΣ** | Πρόχειρος Διαγωνισμός με κριτήριο ανάθεσης την πλέον συμφέρουσα από οικονομικής άποψης προσφορά |
| **ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ** | Σαράντα οχτώ χιλιάδες ευρώ (48.000€), μη συμπεριλαμβανομένου του ΦΠΑ 24%, ύψους έντεκα χιλιάδων πεντακοσίων είκοσι ευρώ (11.520€), δηλαδή πενήντα εννέα χιλιάδες πεντακόσια είκοσι ευρώ (**59.520€**) συμπεριλαμβανομένου του ΦΠΑ 24%,πλέον επτά χιλιάδες ευρώ (7.000€), μη συμπεριλαμβανομένου του ΦΠΑ 24%, ύψους χιλίων εξακοσίων ογδόντα ευρώ (1.680€), δηλαδή πλέον οκτώ χιλιάδων εξακοσίων ογδόντα ευρώ **(8.680€)** σε περίπτωση ενεργοποίησης του δικαιώματος προαίρεσης.  |
| **ΔΙΚΑΙΩΜΑ ΠΡΟΑΙΡΕΣΗΣ** | Παροχή συμβουλευτικών υπηρεσιών να υποστηρίξει τη Βουλή των Ελλήνων κατά την πιστοποίησή της από διαπιστευμένο Φορέα Πιστοποίησης που θα επιλέξει η Βουλή των Ελλήνων |
| **ΔΙΑΡΚΕΙΑ ΣΥΜΒΑΣΗΣ** | Εννέα (9) μήνες από την υπογραφή της |
|  |  |
| **ΚΑΤΑΛΗΚΤΙΚΗ ΗΜΕΡΟΜΗΝΙΑ ΚΑΙ ΩΡΑ ΥΠΟΒΟΛΗΣ ΠΡΟΣΦΟΡΩΝ** | **Τρίτη 07 Μαρτίου** |
| **ΤΟΠΟΣ ΚΑΤΑΘΕΣΗΣ ΠΡΟΣΦΟΡΩΝ** | ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ, Βασ. Σοφίας 11, ΤΚ 106 71 Αθήνα, Τμήμα Γραμματείας, 3ος όροφος, γραφ. 305, από 09:00 έως 13:30. |
| **ΗΜΕΡΟΜΗΝΙΑ ΚΑΙ ΩΡΑ ΑΠΟΣΦΡΑΓΙΣΗΣ ΠΡΟΣΦΟΡΩΝ** | **Τετάρτη 08η Μαρτίου**, και ώρα 11.00, στην αίθουσα 420 (4ος όροφος), Βασ. Σοφίας 11 Αθήνα |

ΘΕΜΑ: Επιλογή αναδόχου για την παροχή συμβουλευτικών υπηρεσιών για την ανάπτυξη και εφαρμογή Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) κατά ISO/ IEC 27001:2013, σύμφωνα με τις τεχνικές και λειτουργικές απαιτήσεις και με κριτήριο ανάθεσης την πλέον συμφέρουσα από οικονομικής άποψης προσφορά,

**ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΕΡΓΟΥ-ΤΕΧΝΙΚΕΣ ΚΑΙ ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ**

## Σκοπός του έργου

Η ανάπτυξη Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών στη Βουλή των Ελλήνων, ώστε να καταστεί εν συνεχεία εφικτή η πιστοποίηση των πληροφοριακών συστημάτων που περιέχονται στο πεδίο εφαρμογής του παρόντος έργου, κατά ISO/IEC 27001:2013.

## Αντικείμενο του έργου

α) Η παροχή εξειδικευμένων υπηρεσιών συμβούλου για το σχεδιασμό, την εγκατάσταση και τη θέση σε λειτουργία Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) κατά ISO/ IEC 27001:2013, με πεδίο εφαρμογής όλες τις δραστηριότητες και τις σχετικές πληροφορίες της Βουλής των Ελλήνων.

β) Η καταγραφή, μελέτη και αξιολόγηση των εφαρμοζόμενων στην Βουλή των Ελλήνων πολιτικών ασφαλείας και πρόταση για την αναθεώρηση και αναβάθμισή τους, σύμφωνα με τα διεθνή πρότυπα και τις βέλτιστες πρακτικές, αλλά και των εθνικών προτύπων και κανόνων για τους κυβερνητικούς οργανισμούς.

γ) Η Αξιολόγηση Επικινδυνότητας, βασιζόμενη σε πρότυπη αναγνωρισμένη μέθοδο, προκειμένου να εντοπιστούν αδυναμίες και ευάλωτα σημεία στις διαδικασίες και στις υποδομές της Βουλής.

δ) Η τεχνική και διοικητική εκπαίδευση του αρμόδιου στελεχιακού δυναμικού της ΒτΕ στην ασφάλεια των πληροφοριών και στις νέες διαδικασίες και πρακτικές, ώστε να είναι σε θέση να διαχειριστεί το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών και μετά τη λήξη του έργου.

Ειδικά, για το μέρος β) του έργου θα πρέπει:

1. Να καταγραφούν αναλυτικά οι εφαρμοζόμενες πολιτικές ασφάλειας και να αναλυθούν τα πλεονεκτήματα και τα μειονεκτήματα, που αυτές παρουσιάζουν.
2. Να εντοπιστούν τυχόν κενά, αλλά και αποκλίσεις από τις συνήθεις πρακτικές, που εφαρμόζονται βάσει των διεθνών προτύπων, αλλά και κοινά αποδεκτών πολιτικών ασφαλείας σε εθνικό, Ευρωπαϊκό και διεθνές επίπεδο, ώστε για τη σύνταξη της νέας πολιτικής να εντοπιστούν και να αξιολογηθούν οι βέλτιστες πρακτικές, που έχουν υιοθετηθεί από άλλους κυβερνητικούς οργανισμούς.
3. Να γίνει μία αναλυτική εσωτερική περιγραφή τού τι ακριβώς θα πρέπει να ασφαλιστεί και από τι. Πλην των εξωτερικών επιθέσεων, θα πρέπει να αντιμετωπιστεί και το ενδεχόμενο ζημιών από πιθανό εσωτερικό λάθος ή μη ορθή χρήση από τους εσωτερικούς χρήστες ή κακόβουλες ενέργειες από το εσωτερικό περιβάλλον (insider threats).

## Δικαίωμα Προαίρεσης

Σε περίπτωση ενεργοποίησης του δικαιώματος προαίρεσης προβλέπεται η δυνατότητα να ζητηθεί από τον ανάδοχο, η υποστήριξη των διαδικασιών που θα πραγματοποιήσει η Βουλή των Ελλήνων κατά την πιστοποίησή της από διαπιστευμένο Φορέα Πιστοποίησης, ώστε να καταστεί εφικτή η πιστοποίηση των πληροφοριακών συστημάτων που περιέχονται στο πεδίο εφαρμογής του παρόντος έργου, κατά ISO/IEC 27001:2013.

Το δικαίωμα προαίρεσης δύναται να ασκηθεί μετά από έγγραφο αίτημα της αναθέτουσας αρχής έως και δώδεκα (12) μήνες μετά την οριστική παραλαβή του έργου.

## Διαστασιολόγηση του έργου

Στα πλαίσια της προετοιμασίας για την ανάπτυξη του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, ο Σύμβουλος θα πρέπει να συνεργαστεί με τα στελέχη της Βουλής των Ελλήνων προκειμένου να προσδιορίσει και να περιλάβει στο αντικείμενο του έργου τους πόρους που σχετίζονται με τις επιχειρησιακές λειτουργίες των σαράντα (40) κρίσιμων οργανικών μονάδων του οργανισμού, όπως καθορίζονται από τον οργανισμό.

Το σύνολο των κρίσιμων πληροφοριακών πόρων του οργανισμού, ανέρχεται σε πενήντα (50) εφαρμογές οι οποίες εξυπηρετούνται από περίπου 200 εξυπηρετητές/servers και οι οποίοι είναι κατανεμημένοι σε 7 data centers.

Επιπρόσθετα, ο Σύμβουλος θα προσδιορίσει τις ανάγκες προστασίας των πληροφοριών που τηρούνται ή διακινούνται μέσω των πληροφοριακών υποδομών της Βουλής, θα ορίσει τα αναγκαία επίπεδα διαβάθμισής τους, τα απαραίτητα μέτρα προστασίας τους, τις επιτρεπτές ενέργειες χειρισμού τους από τους εργαζόμενους και τους συνεργάτες της Βουλής και θα αναπτύξει τις αντίστοιχες διαδικασίες.

Επίσης ο Σύμβουλος θα προχωρήσει σε χαρτογράφηση της διαχείρισης των προσωπικών και των ευαίσθητων δεδομένων από την Βουλή των Ελλήνων,  με σκοπό να καταγραφεί ποια προσωπικά και ευαίσθητα δεδομένα συλλέγονται, υπόκεινται σε επεξεργασία, οι σκοποί της επεξεργασίας για τους οποίους συλλέγονται τα δεδομένα, το χρονικό διάστημα που διατηρούνται, ποιος έχει πρόσβαση στα δεδομένα, πως προστατεύονται, σε ποιους συνεργάτες διαβιβάζονται και για ποιους σκοπούς. Ο Σύμβουλος θα πρέπει να υποδείξει σχετικούς τρόπους και διαδικασίες που θα πρέπει να εφαρμόζονται από όλους αυτούς που συλλέγουν, επεξεργάζονται και γενικότερα διαχειρίζονται τα ως άνω δεδομένα, λαμβάνοντας υπόψη του και το νέο Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου ο οποίος τίθεται σε ισχύ το 2018.

## Ελάχιστες Προϋποθέσεις Συμμετοχής

Δικαίωμα συμμετοχής έχουν:

α) φυσικά ή νομικά πρόσωπα

β) ενώσεις προμηθευτών που υποβάλλουν κοινή προσφορά

γ) συνεταιρισμοί

δ) κοινοπραξίες προμηθευτών.

Ο υποψήφιος ανάδοχος πρέπει:

1. Να διαθέτει την κατάλληλη οργάνωση, δομή και μέσα, ώστε να ανταπεξέλθει επιτυχώς στις απαιτήσεις του έργου.

Ο υποψήφιος ανάδοχος οφείλει να αποδείξει τα ανωτέρω, καταθέτοντας με την προσφορά του αναλυτικές πληροφορίες, σχετικά με:

* την οργανωτική του δομή, τις εγκαταστάσεις και τον εξοπλισμό που διαθέτει, με ιδιαίτερη αναφορά στη μηχανοργάνωσή του.
* τις συνεργασίες με εξωτερικούς προμηθευτές, κανάλια εξυπηρέτησης,
* τους τομείς δραστηριότητας και τους κλάδους εξειδίκευσης
* τα προϊόντα και υπηρεσίες που παρέχει
* τη μεθοδολογία, τα εργαλεία και τις τεχνικές που χρησιμοποιεί για την υλοποίηση του έργου με σαφή αναφορά στις οντότητες (π.χ. Τμήματα, Μονάδες, Υπηρεσίες) οι οποίες καλύπτουν την ανωτέρω προϋπόθεση συμμετοχής.
1. Να διαθέτει πιστοποίηση κατά ISO 9001:2008 και ISO 27001:2013 με πεδίο εφαρμογής την παροχή συμβουλευτικών υπηρεσιών.
2. Να διαθέτει ανθρώπινο δυναμικό και πόρους ικανούς και αξιόπιστους για να φέρει σε πέρας επιτυχώς τις απαιτήσεις του έργου, σε όρους απαιτούμενης εξειδίκευσης, επαγγελματικών προσόντων και εμπειρίας.

Συγκεκριμένα απαιτείται κατ’ ελάχιστον:

* Να διαθέτει επιστημονικό υπεύθυνο, με μεταπτυχιακό τίτλο σπουδών στον τομέα της Πληροφορικής/Πληροφοριακών Συστημάτων/Ασφάλειας Πληροφοριακών Συστημάτων και Δικτύων/Τεχνολογιών ΤΠΕ ή συναφούς αντικειμένου και με αποδεικνυόμενη πενταετή (5) εμπειρία σε σχετικά έργα, ο οποίος θα έχει την ευθύνη σύνταξης των ζητούμενων μελετών.
* Να διαθέτει υπεύθυνο έργου (project manager) με μεταπτυχιακό τίτλο σπουδών στον τομέα της Πληροφορικής/Πληροφοριακών Συστημάτων/Ασφάλειας Πληροφοριακών Συστημάτων και Δικτύων/Τεχνολογιών ΤΠΕ ή συναφούς αντικειμένου και με αποδεικνυόμενη κατ’ ελάχιστο πενταετή (5) εμπειρία, που θα αναλάβει τον συντονισμό των εργασιών που προβλέπονται για την υλοποίηση του υπό προκήρυξη έργου.
* Τα στελέχη του αναδόχου που θα λάβουν μέρος στο έργο θα πρέπει να διαθέτουν προπτυχιακό ή μεταπτυχιακό τίτλο σπουδών στον τομέα της Πληροφορικής/Πληροφοριακών Συστημάτων/Ασφάλειας Πληροφοριακών Συστημάτων και Δικτύων/Τεχνολογιών ΤΠΕ ή συναφούς αντικειμένου και αποδεικνυόμενη εμπειρία σε σχετικά έργα.
* Στην προσφορά του αναδόχου θα πρέπει υποχρεωτικά να περιλαμβάνονται αναλυτικά Βιογραφικά Σημειώματα του υπεύθυνου έργου, του επιστημονικού υπεύθυνου, καθώς και των στελεχών του αναδόχου που θα λάβουν μέρος στο έργο, από τα οποία να αποδεικνύεται ευθέως και χωρίς άλλη αναγκαία πληροφορία ή διευκρίνιση, η εξειδίκευση, τα επαγγελματικά προσόντα και η εμπειρία τους, σχετικά με τις απαιτήσεις που αναλαμβάνουν, όπως προκύπτει από τον ρόλο τους στο έργο.
* Σε περίπτωση που ο προτεινόμενος υπεύθυνος του έργου ή/και τα λοιπά στελέχη δεν είναι μόνιμα στελέχη του υποψηφίου αναδόχου, αλλά εξωτερικοί συνεργάτες, η πρόταση πρέπει να συνοδεύεται από υπεύθυνες δηλώσεις τους ότι υπάρχει συμφωνία συνεργασίας για όλη την προβλεπόμενη διάρκεια της σύμβασης και ότι είναι αποδεκτοί οι όροι του παρόντος διαγωνισμού.

## Οι φάσεις υλοποίησης του έργου

Φάση Α – Καταγραφή και αξιολόγηση υφιστάμενης κατάστασης

* Ο σύμβουλος θα αναλάβει την εκπόνηση διαγνωστικής μελέτης στις υφιστάμενες διαδικασίες και πληροφοριακές υποδομές της Βουλής των Ελλήνων, με σκοπό τον εντοπισμό των απαραίτητων ενεργειών για τη συμμόρφωση με το ISO 27001.
* Η διαγνωστική έκθεση του συμβούλου θα περιλαμβάνει:
	+ αποκλίσεις στις υφιστάμενες διαδικασίες και υποδομές από τα προβλεπόμενα στο πρότυπο ISO/ IEC 27001:2013
	+ προτάσεις/απαιτούμενες ενέργειες με χρονοδιάγραμμα και υπευθυνότητες για τη βελτίωση/ άρση των αποκλίσεων.

Φάση Β – Διενέργεια Αξιολόγησης Επικινδυνότητας, βασιζόμενη σε πρότυπη αναγνωρισμένη μέθοδο, προκειμένου να εντοπιστούν αδυναμίες και ευάλωτα σημεία στις διαδικασίες και στις υποδομές του οργανισμού.

* Στη φάση αυτή, ο σύμβουλος θα αναλάβει την διενέργεια Αξιολόγησης Επικινδυνότητας, η οποία θα περιλαμβάνει τουλάχιστον τα εξής:
	+ Αποτύπωση των απειλών που αντιμετωπίζουν τα συστήματα του οργανισμού
	+ Αξιολόγηση του ρίσκου που τα συστήματα του οργανισμού αντιμετωπίζουν σε συνάρτηση με τις απειλές και την επίπτωση αυτών στην ακεραιότητα, την εμπιστευτικότητα και την διαθεσιμότητα των πληροφοριών που αυτά διαχειρίζονται
	+ Καθορισμός των προτεινόμενων σημείων ελέγχου ώστε να περιοριστεί το ανώτερο ρίσκο σε αποδεκτά επίπεδα
	+ Πρόταση πλάνου ενεργειών για την υλοποίηση των παραπάνω σημείων ελέγχου

Φάση Γ – Σχεδιασμός και ανάπτυξη του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ)

* Στη φάση αυτή, ο σύμβουλος θα αναλάβει το σχεδιασμό της απαιτούμενης τεκμηρίωσης του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, η οποία θα περιλαμβάνει τουλάχιστον τα εξής:
	+ Πολιτικές Ασφάλειας Πληροφοριών
	+ Περιγραφές Θέσεων Εργασίας σε σχέση με τις αρμοδιότητες και τις ευθύνες αυτών σχετικά με την ασφάλεια των πληροφοριών
	+ Αξιολόγηση Επικινδυνότητας (risk assessment)
	+ Εγχειρίδιο Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
	+ Διαδικασίες Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
	+ Αρχεία του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

Θα συνεκτιμηθεί η εγκατάσταση λογισμικού για την ηλεκτρονική διαχείριση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, προκειμένου να αυτοματοποιηθούν οι διοικητικές απαιτήσεις του: έλεγχος εγγράφων, αξιολόγηση προμηθευτών, διαχείριση μη συμμορφώσεων, εσωτερικές επιθεωρήσεις, διορθωτικές ενέργειες, εκπαίδευση προσωπικού, ανασκόπηση από τη διοίκηση.

Στη φάση αυτή ο σύμβουλος θα συγγράψει την απαραίτητη τεκμηρίωση που περιγράφεται στη φάση Γ, λαμβάνοντας υπόψη την υπάρχουσα διαδικασία κωδικοποίησης και αρχειοθέτησης εγγράφων. Επιπρόσθετα θα γίνει χρήση των υφισταμένων προτύπων (templates) με σκοπό την ομαλή ένταξη με το τρέχον σύστημα τεκμηρίωσης.

Φάση Δ – Εκπαίδευση εφαρμογής

* Στη φάση αυτή, ο Σύμβουλος θα αναλάβει την εκπαίδευση του αρμόδιου στελεχιακού δυναμικού της Βουλής των Ελλήνων, ώστε να είναι σε θέση να εφαρμόσει το Σύστημα και μετά την πιστοποίησή του.

Συγκεκριμένα, ο Σύμβουλος θα υλοποιήσει κατ’ ελάχιστον τρία εκπαιδευτικά προγράμματα, με αντικείμενο:

1. Εκπαίδευση εκπαιδευτών (train the trainer), διάρκειας οκτώ (8) ωρών, για μία ομάδα δώδεκα (12) στελεχών, με κάλυψη κατ’ ελάχιστον των εξής θεματικών ενοτήτων: είδη απειλών και κινδύνων εντός και εκτός του οργανισμού, διεθνείς πρακτικές και τεχνολογίες για την αντιμετώπιση απειλών, case studies και επίδειξη δικτυακών επιθέσεων και περιστατικών ασφαλείας, κλπ
2. Εκπαίδευση επί των γενικών αρχών ασφάλειας πληροφοριών, της εφαρμογής των Διαδικασιών και της συμπλήρωσης των απαιτούμενων αρχείων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, διάρκειας οκτώ (8) ωρών, για 40 στελέχη του οργανισμού, χωρισμένα σε 2 ομάδες
3. Εκπαίδευση Εσωτερικών Επιθεωρητών Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών, διάρκειας οκτώ (8) ωρών, για μία ομάδα δώδεκα (12) στελεχών
* Ο σύμβουλος θα παραδώσει στη Βουλή των Ελλήνων το εκπαιδευτικό υλικό (παρουσιάσεις, σημειώσεις, case studies) σε έντυπη και ηλεκτρονική μορφή, καθώς και πιστοποιητικά εκπαίδευσης ανά συμμετέχοντα.

Φάση Ε – Πιλοτική εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών

* Η φάση αυτή περιλαμβάνει την υποστήριξη, από την πλευρά του Συμβούλου, για την πιλοτική εφαρμογή του Συστήματος, τον εντοπισμό τυχόν προβλημάτων στην εφαρμογή του, την υποβολή προτάσεων διορθωτικών ενεργειών και την οριστικοποίηση της τεκμηρίωσης του Συστήματος. Σκοπός της φάσης αυτής είναι η ολοκλήρωση ενός πλήρους κύκλου ζωής του ΣΔΑΠ (Plan-Do-Check-Act), ώστε να εφαρμόσουν στην πράξη τα στελέχη και το προσωπικό της Βουλής των Ελλήνων όσα διδάχθηκαν στην προηγούμενη φάση της εκπαίδευσης, να αναγνωρισθούν τυχόν παραλείψεις, δυσκολίες στην εφαρμογή των Διαδικασιών του ΣΔΑΠ και να αντιμετωπιστούν. Τα στελέχη και το προσωπικό της Βουλής των Ελλήνων θα πρέπει να ενσωματώσουν στην καθημερινή τους εργασία πρακτικές ασφαλείας που θα έχουν οριστεί στις Πολιτικές Ασφάλειας Πληροφοριών.

Για το λόγο αυτό, ο σύμβουλος θα αναλάβει τη διενέργεια ελέγχων/ επιθεωρήσεων με σκοπό τη βελτιστοποίηση της εφαρμογής και θα παρέχει τεχνική βοήθεια για την εφαρμογή των διαδικασιών του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Οι εκπαιδευμένοι κατά την προηγούμενη φάση Εσωτερικοί Επιθεωρητές θα συμμετέχουν στις εσωτερικές επιθεωρήσεις που θα υλοποιήσει ο σύμβουλος. Με το πέρας των εσωτερικών επιθεωρήσεων, ο σύμβουλος θα συντάξει και θα υποβάλει αναφορά, η οποία μεταξύ άλλων θα περιλαμβάνει, όπου απαιτείται, διορθωτικές ενέργειες και προτάσεις βελτίωσης του ΣΔΑΠ.

* Επιπλέον, στη φάση αυτή, ο Σύμβουλος θα αναλάβει την προετοιμασία του φακέλου/ αίτησης που θα υποβληθεί προς τον αρμόδιο Φορέα Πιστοποίησης.

**Προαίρεση**

Ο σύμβουλος αναλαμβάνει την υποχρέωση να υποστηρίξει τη Βουλή των Ελλήνων κατά την πιστοποίησή της από διαπιστευμένο Φορέα Πιστοποίησης που θα επιλέξει η Βουλή των Ελλήνων, και συγκεκριμένα:

* θα παρίσταται κατά την επιθεώρηση του Φορέα Πιστοποίησης
* θα υποβάλει προτάσεις για την άρση τυχόν μη συμμορφώσεων / παρατηρήσεων που προκύψουν κατά τη διάρκεια της επιθεώρησης πιστοποίησης.

## Χρονοδιάγραμμα υλοποίησης του έργου

Ο συνολικός χρόνος υλοποίησης του έργου δεν θα πρέπει να υπερβεί τους εννιά (9) μήνες και θα πρέπει να κατανεμηθεί στις παρακάτω φάσεις:

|  |  |
| --- | --- |
| **Φάση** |  |
| **Oμάδα 1** |  |
| **Φάση Α** – Καταγραφή και αξιολόγηση υφιστάμενης κατάστασης |  |
| **Φάση Β** – Διενέργεια Αξιολόγησης Επικινδυνότητας, |  |
| **Φάση Γ** – Σχεδιασμός και ανάπτυξη του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών  |  |
| **Φάση Δ** – Εκπαίδευση εφαρμογής  |  |
| **Φάση Ε** – Πιλοτική εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών  |  |

Οι προσφορές των υποψηφίων θα πρέπει να περιλαμβάνουν κατ’ ελάχιστον:

* τη μεθοδολογία υλοποίησης του έργου
* τα παραδοτέα του έργου
* κρίσιμα σημεία (milestones)
* αναλυτικό χρονοδιάγραμμα υλοποίησης
* λίστα προτεινόμενων Διαδικασιών
* manual του προτεινόμενου λογισμικού
* αναλυτικό εκπαιδευτικό πρόγραμμα σεμιναρίων
* εμπλεκόμενα στελέχη από πλευράς του οργανισμού και εκτιμώμενο χρόνο απασχόλησης
* αμοιβή για τις υπηρεσίες (Οικονομική Προσφορά)

Γίνονται δεκτές προσφορές που καλύπτουν το σύνολο του έργου συν την προαίρεση. Εναλλακτικές προσφορές δεν γίνονται δεκτές, είτε στο σύνολο του έργου, είτε στα επιμέρους τμήματά του.

## Αξιολόγηση προσφορών

Οι προσφορές θα πρέπει να περιλαμβάνουν την αναλυτική μεθοδολογία υλοποίησης του έργου, τα παραδοτέα του έργου, αναλυτικά προγράμματα εκπαίδευσης του προσωπικού, μεθοδολογία και εργαλεία του τεχνικού ελέγχου ασφάλειας πληροφοριακών συστημάτων για την εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με το Διεθνές Πρότυπο ISO/IEC 27001:2013 στη Βουλή των Ελλήνων.

Το κριτήριο επιλογής Αναδόχου και κατακύρωσης του έργου σε αυτόν είναι η πλέον συμφέρουσα από οικονομικής άποψης προσφορά.

Δικαίωμα αξιολόγησης της τεχνικής και οικονομικής προσφοράς διατηρούν μόνο οι υποψήφιοι που κρίνονται ποιοτικά επαρκείς σύμφωνα με τα όσα ορίζονται στην παρούσα.

Η πλέον συμφέρουσα από οικονομικής άποψης προσφορά είναι εκείνη που παρουσιάζει το μεγαλύτερο Λj, όπου το Λj υπολογίζεται για κάθε προσφορά από τον ακόλουθο τύπο:

Λj = 80\*(Tj/Tmax) +20 \* (Kmin/Kj)

όπου:

Kj = Κόστος Προσφοράς,

Kmin = Κόστος της χαμηλότερης προσφοράς (μικρότερο κόστος),

Tj = Συνολική Βαθμολογία Τεχνικών Κριτηρίων Αξιολόγησης προσφοράς

Tmax = Συνολική Βαθμολογία Τεχνικών Κριτηρίων της αξιολογηθείσας ως καλύτερη προσφορά (αυτή που συγκέντρωσε τη μεγαλύτερη βαθμολογία).

Ως πλέον συμφέρουσα από οικονομικής άποψης προσφορά ανακηρύσσεται αυτή που παρουσιάζει το μέγιστο Λj στον παραπάνω τύπο. Ο υπολογισμός του Λj γίνεται μέχρι το τρίτο δεκαδικό ψηφίο, χωρίς στρογγυλοποίηση. Σε περίπτωση ισοβαθμίας υπολογίζονται και τα υπόλοιπα δεκαδικά ψηφία του αποτελέσματος.

Η βαθμολογία των επιμέρους κριτηρίων, είναι οι 100 βαθμοί, για τις περιπτώσεις που καλύπτονται πλήρως όλες οι απαιτήσεις των τεχνικών προδιαγραφών των προσφορών, που απεικονίζονται στα επιμέρους κριτήρια.

Η βαθμολογία αυτή αυξάνεται έως τους 110 βαθμούς, όταν οι προσφορές υπερκαλύπτουν τις τεχνικές προδιαγραφές που αξιολογούνται με τα επιμέρους κριτήρια.

Κόστος προσφοράς,  θα θεωρείται η συνολική τιμή για το έργο η οποία θα περιλαμβάνει όλες τις σχετικές εργασίες μελέτης, ανάλυσης και παραδοτέων ανά φάση καθώς και το κόστος της προαίρεσης.

Τα κριτήρια τεχνικής αξιολόγησης και οι αντίστοιχοι συντελεστές βαρύτητας δίνονται στον παρακάτω πίνακα:

|  |  |  |
| --- | --- | --- |
| **αα** | **Κριτήριο** | **Συντελεστής βαρύτητας** |
| 1 | Κατανόηση του αντικειμένου, των αναγκών, των απαιτήσεων και των ιδιαίτερων προβλημάτων του έργου | 20% |
| 2 | Αναλυτική περιγραφή μεθοδολογίας υλοποίησης του Έργου. Σαφήνεια φάσεων και παραδοτέων του Έργου | 40% |
| 3 | Εφικτότητα και ρεαλιστικότητα του χρονοπρογραμματισμού των εργασιών | 15% |
| 4 | Δομή και σύνθεση της ομάδας έργου του αναδόχου, αποτελεσματικότητα διαδικασιών επικοινωνίας με την αναθέτουσα αρχή και διασφάλισης της ποιότητας του έργου | 25% |

## Οικονομική Προσφορά

Στην Οικονομική Προσφορά θα πρέπει η τιμή να δίνεται για το έργο και την προαίρεση ξεχωριστά, καθώς και για το σύνολο του έργου σε ΕΥΡΩ.

Το συμβατικό τίμημα για την εκτέλεση του έργου από τον ανάδοχο ανέρχεται στο ποσό των …………………….ευρώ, πλέον του ΦΠΑ

Στην περίπτωση ενεργοποίησης της προαίρεσης το συμβατικό τίμημα ανέρχεται στο ποσό των …………………………….πλέον του ΦΠΑ

## Πίνακας Συμμόρφωσης

 Ο υποψήφιος Ανάδοχος συμπληρώνει τον πίνακα συμμόρφωσης με την απόλυτη ευθύνη της ακρίβειας των δεδομένων

| **Α/Α** | **ΠΕΡΙΓΡΑΦΗ** | **ΥΠΟΧΡΕΩΤΙΚΗ ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ** |
| --- | --- | --- | --- | --- |
| **ΑΝΑΣΚΟΠΗΣΗ ΚΑΙ ΑΝΑΒΑΘΜΙΣΗ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ** |
|  | Πλήρης μελέτη και αξιολόγηση των εφαρμοζόμενων πολιτικών ασφαλείας με βάση το ISO/IEC 27000:2013 Family of Standards | ΝΑΙ |  |  |
|  | Καταγραφή αναλυτικά των εφαρμοζόμενων στην Βουλή των Ελλήνων πολιτικών ασφάλειας | ΝΑΙ |  |  |
|  | Ανάλυση των πλεονεκτημάτων και των μειονεκτημάτων των εφαρμοζόμενων πολιτικών | NAI |  |  |
|  | Εντοπισμός κενών και αποκλίσεων από τις συνήθεις πρακτικές. | ΝΑΙ |  |  |
|  | Εκτενής μελέτη των διεθνών προτύπων, αλλά κοινά αποδεκτών πολιτικών ασφαλείας σε εθνικό, Ευρωπαϊκό και διεθνές επίπεδο, με στόχο να εντοπιστούν και να αξιολογηθούν οι βέλτιστες πρακτικές, που έχουν υιοθετηθεί από άλλες στατιστικές υπηρεσίες και κυβερνητικούς οργανισμούς, σύμφωνα με το μοντέλο ISMS | ΝΑΙ |  |  |
|  | Χαρτογράφηση της διαχείρισης των προσωπικών και ευαίσθητων δεδομένων από την Βουλή των Ελλήνων,  με σκοπό να καταγραφούν ποια προσωπικά και ευαίσθητα δεδομένα συλλέγονται, υπόκεινται σε επεξεργασία, οι σκοποί της επεξεργασίας για τους οποίους συλλέγονται τα δεδομένα, το χρονικό διάστημα που διατηρούνται, ποιος έχει πρόσβαση στα δεδομένα, πως προστατεύονται, σε ποιους συνεργάτες διαβιβάζονται και για ποιους σκοπούς.Να υποδειχθούν σχετικοί τρόποι και διαδικασίες που θα πρέπει να εφαρμόζονται από όλους αυτούς που συλλέγουν, επεξεργάζονται και γενικότερα διαχειρίζονται τα ως άνω δεδομένα, λαμβάνοντας υπόψη και το νέο Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου ο οποίος τίθεται σε ισχύ το 2018. | ΝΑΙ |  |  |
|  | Προσδιορισμός αναγκών προστασίας των πληροφοριών που τηρούνται ή διακινούνται μέσω των πληροφοριακών υποδομών της Βουλής, καθορισμός αναγκαίων επιπέδων διαβάθμισής τους, απαραίτητων μέτρων προστασίας τους, επιτρεπτές ενέργειες χειρισμού τους από τους εργαζόμενους και τους συνεργάτες της Βουλής και ανάπτυξη αντίστοιχων διαδικασιών | ΝΑΙ |  |  |
|  | Εντοπισμός αποκλίσεων ανάμεσα στις ισχύουσες πολιτικές ασφάλειας στην Βουλή των Ελλήνων και στις διεθνείς πρακτικές και σχεδιασμός μέτρων για να εξομαλυνθούν οι αποκλίσεις και διαφορές | ΝΑΙ |  |  |
| **ΜΕΛΕΤΗ ΑΠΟΤΙΜΗΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ (RISK ASSESSMENT):** |
|  | Ο Ανάδοχος θα πρέπει να εκπονήσει μελέτη αποτίμησης της επικινδυνότητας, προκειμένου να εντοπιστούν και να μετριαστούν οι απειλές, τα τρωτά σημεία και οι πιθανές επιπτώσεις, και τελικά να αποτιμηθούν οι κίνδυνοι ασφαλείας που αντιμετωπίζει η Βουλή των Ελλήνων . | ΝΑΙ |  |  |
|  | Να γίνει αποτίμηση της αξίας των αγαθών | ΝΑΙ |  |  |
|  | Να εντοπιστούν οι αδυναμίες και να περιγραφούν οι επιπτώσεις και οι συνέπειες που θα επιφέρει ένα ενδεχόμενο περιστατικό ασφάλειας ή ενδεχόμενη απειλή. | ΝΑΙ |  |  |
|  | Να αποτιμηθεί η επικινδυνότητα (risk assessment) των συστημάτων, εφαρμογών και εγκαταστάσεων  | ΝΑΙ |  |  |
|  | Να γίνει μεθοδικός εντοπισμός και περιγραφή με σαφήνεια των μέτρων ασφαλείας που πρέπει να ληφθούν για την επαρκή προστασία των συστημάτων. | ΝΑΙ |  |  |
|  | Η μέθοδος που θα χρησιμοποιηθεί στη διαδικασία της Μελέτης Αποτίμησης Επικινδυνότητας θα πρέπει να είναι συστηματική, ευρείας επιστημονικής και επαγγελματικής αποδοχής (σε εθνική ή σε διεθνή κλίμακα). | ΝΑΙ |  |  |
|  | Να υποστηρίζεται από αυτοματοποιημένο εργαλείο, το οποίο να υλοποιεί τις επιμέρους φάσεις και τα βήματα της μεθοδολογίας. | ΝΑΙ |  |  |
|  | Να είναι συμβατή με το ISMS - πρότυπο ΙSO/IEC 27000:2013 series (Family of Standards) | ΝΑΙ |  |  |
|  | Να καλύπτει όλες τις συνιστώσες της ασφάλειας, περιλαμβανομένων του τεχνικού παράγοντα, των θεμάτων διαδικασιών και προσωπικού, της ασφάλειας δικτύων κ.λπ. | ΝΑΙ |  |  |
| **Σχεδιασμός και ανάπτυξη του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών** |
|  | Η απαιτούμενη τεκμηρίωσης του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, θα περιλαμβάνει τουλάχιστον τα εξής:* Πολιτικές Ασφάλειας Πληροφοριών
* Περιγραφές Θέσεων Εργασίας σε σχέση με τις αρμοδιότητες και τις ευθύνες αυτών σχετικά με την ασφάλεια των πληροφοριών
* Αξιολόγηση Επικινδυνότητας (risk assessment)
* Εγχειρίδιο Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
* Διαδικασίες Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
* Αρχεία του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.
 | ΝΑΙ |  |  |
|  | Χρήση της υφιστάμενης διαδικασίας κωδικοποίησης και αρχειοθέτησης εγγράφων | ΝΑΙ |  |  |
|  | Χαρακτηριστικά του παραδοτέου:* Σαφήνεια και εύκολη κατανόηση: απευθύνεται στο σύνολο των χρηστών της ΒτΕ, θα πρέπει συνεπώς να είναι κατανοητή απ’ όλους
* Τεχνολογική ανεξαρτησία: Να μη δεσμεύει την ΒτΕ σε συγκεκριμένα προϊόντα και τεχνολογίες
* Καταλληλότητα: να καλύπτει τις ανάγκες της συγκεκριμένης Υπηρεσίας
* Εφαρμοσιμότητα: Τα μέτρα που θα προβλέπει, θα πρέπει να μπορούν να εφαρμόζονται, χωρίς να δυσχεραίνουν δυσανάλογα τις δραστηριότητες των χρηστών
 | ΝΑΙ |  |  |
|  | Η μελέτη θα επικεντρωθεί τόσο σε θέματα εξοπλισμού (hardware), όσο και σε θέματα διαδικασιών ασφάλειας (procedures) των συστημάτων πληροφορικής της Βουλής των Ελλήνων και θα συμπεριλαμβάνει την πολιτική ασφαλείας, την αξιολόγηση επικινδυνότητας, την πολιτική αντιμετώπισης συμβάντων ασφαλείας και τους προβλεπόμενους ελέγχους, ώστε να συγκροτεί ένα Ολοκληρωμένο Σύστημα Διαχείρισης Ασφαλείας (Integrated Security Management System), σύμφωνα προς το διεθνές πρότυπο ISO 27000:2013, ISMS Family of Standards. | ΝΑΙ |  |  |
| **Εκπαίδευση εφαρμογής** |
|  | Εκπαίδευση εκπαιδευτών (train the trainer), διάρκειας οκτώ (8) ωρών, για μία ομάδα δώδεκα (12) στελεχών, με κάλυψη κατ’ ελάχιστον των εξής θεματικών ενοτήτων: είδη απειλών και κινδύνων εντός και εκτός του οργανισμού, διεθνείς πρακτικές και τεχνολογίες για την αντιμετώπιση απειλών, case studies και επίδειξη δικτυακών επιθέσεων και περιστατικών ασφαλείας | ΝΑΙ |  |  |
|  | Εκπαίδευση επί των γενικών αρχών ασφάλειας πληροφοριών, της εφαρμογής των Διαδικασιών και της συμπλήρωσης των απαιτούμενων αρχείων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, διάρκειας οκτώ (8) ωρών, για 40 στελέχη του οργανισμού, χωρισμένα σε 2 ομάδες | ΝΑΙ |  |  |
|  | Εκπαίδευση Εσωτερικών Επιθεωρητών Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών, διάρκειας οκτώ (8) ωρών, για μία ομάδα δώδεκα (12) στελεχών | ΝΑΙ |  |  |
|  | Η εκπαίδευση των χρηστών θα πραγματοποιηθεί στους χώρους της Αναθέτουσας Αρχής σε χώρο που θα υποδείξει ο Φορέας | ΝΑΙ |  |  |
| **Πιλοτική εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών** |
|  | Ο ανάδοχος οφείλει να προσφέρει υπηρεσίες πιλοτικής λειτουργίας, διάρκειας τουλάχιστον ενός (1) μηνός.  | ΝΑΙ |  |  |
|  | Κατά τη διάρκεια της πιλοτικής λειτουργίας, ο ανάδοχος οφείλει να προσφέρει καθημερινή επιτόπια παρουσία εξειδικευμένου προσωπικού. | ΝΑΙ |  |  |
|  | ολοκλήρωση ενός πλήρους κύκλου ζωής του ΣΔΑΠ (Plan-Do-Check-Act) | ΝΑΙ |  |  |
|  | Διενέργεια ελέγχων/επιθεωρήσεων με σκοπό τη βελτιστοποίηση της εφαρμογής και θα παρέχει τεχνική βοήθεια για την εφαρμογή των διαδικασιών του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. | ΝΑΙ |  |  |
|  | Με το πέρας των εσωτερικών επιθεωρήσεων, ο σύμβουλος θα συντάξει και θα υποβάλει αναφορά, η οποία μεταξύ άλλων θα περιλαμβάνει, όπου απαιτείται, διορθωτικές ενέργειες και προτάσεις βελτίωσης του ΣΔΑΠ | ΝΑΙ |  |  |
|  | Προετοιμασία του φακέλου/αίτησης που θα υποβληθεί προς τον αρμόδιο Φορέα Πιστοποίησης. | ΝΑΙ |  |  |

**Προαίρεση**

| **Πιστοποίηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών** |
| --- |
| **Α/Α** | **ΠΕΡΙΓΡΑΦΗ** | **ΥΠΟΧΡΕΩΤΙΚΗ ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ** | **ΠΑΡΑΠΟΜΠΗ** |
|  | Ο σύμβουλος αναλαμβάνει την υποχρέωση να υποστηρίξει τη Βουλή των Ελλήνων κατά την πιστοποίησή της από διαπιστευμένο Φορέα Πιστοποίησης | ΝΑΙ |  |  |
|  | Παράσταση σύμβουλου κατά την επιθεώρηση του Φορέα Πιστοποίησης | ΝΑΙ |  |  |
|  | Υποβολή προτάσεων για την άρση τυχόν μη συμμορφώσεων/παρατηρήσεων που πιθανά προκύψουν κατά τη διάρκεια της επιθεώρησης πιστοποίησης | ΝΑΙ |  |  |

 \* Για τη στήλη, ΥΠΟΧΡΕΩΤΙΚΗ ΑΠΑΙΤΗΣΗ, η λέξη "ΝΑΙ" σημαίνει υποχρεωτική προδιαγραφή

Σημείωση: "O Ανάδοχος κατά την υπογραφή της σύμβασης να υπογράψει και σύμβαση εμπιστευτικότητας (NDA) με την Βουλή των Ελλήνων ".