ΠΑΡΑΡΤΗΜΑ ΙΙ

**ΥΠΟΔΕΙΓΜΑ ΦΥΛΛΟΥ ΣΥΜΜΟΡΦΩΣΗΣ**

(Αναλυτικό φύλλο συμμόρφωσης- τεκμηρίωσης, με το οποίο δίνονται αναλυτικές απαντήσεις με σχετικές παραπομπές σε όλα τα σημεία των «Απαιτήσεων- Τεχνικών Προδιαγραφών», καθώς και σε κάθε άλλη τεχνική απαίτηση της Αναθέτουσας Αρχής)

**Υπηρεσίες CISO**

|  |  |  |  |
| --- | --- | --- | --- |
| **ΠΕΡΙΓΡΑΦΗ ΤΕΧΝΙΚΗΣ ΠΡΟΔΙΑΓΡΑΦΗΣ** | **ΑΠΑΙΤΗΣΗ** | **ΑΠΑΝΤΗΣΗ ΥΠΟΨΗΦΙΟΥ** | **ΠΑΡΑΠΟΜΠΗ ΣΕ  ΤΕΧΝΙΚΑ ΦΥΛΛΑΔΙΑ** |
| **Εφαρμογή του Κανονισμού Ασφάλειας Πληροφοριών και Δικτύων** |  |  |  |
| Οι αρμοδιότητες του Υπευθύνου Ασφαλείας Πληροφοριών και Δικτύων θα είναι κατ’ ελάχιστον οι ακόλουθες: | ΝΑΙ |  |  |
| * Να αποτελεί το σημείο επαφής με την Εθνική Αρχή Κυβερνοασφάλειας και το αρμόδιο CSIRT. | ΝΑΙ |  |  |
| * Να συντονίζει και επιβλέπει το Νοσοκομείο ως προς τις υποχρεώσεις που απορρέουν από τον N. 4577/2018, την Yπουργική Aπόφαση 1027/2019 καθώς και από άλλες διατάξεις της Ευρωπαϊκής Ένωσης ή της Εθνικής Αρχής Κυβερνοασφάλειας σχετικά με την Ασφάλεια Συστημάτων Δικτύων και Πληροφοριών. | ΝΑΙ |  |  |
| * Να εποπτεύει την υλοποίηση της Ενιαίας Πολιτικής Ασφάλειας και την ικανοποίηση των βασικών απαιτήσεων ασφάλειας, την εκπαίδευση και ευαισθητοποίηση των υπαλλήλων του Νοσοκομείου σε θέματα ασφάλειας πληροφοριών και δικτύων καθώς, και τη σύνταξη της αναφοράς αυτοαξιολόγησης του Νοσοκομείου που αποστέλλεται στην Εθνική Αρχή Κυβερνοσφάλειας. | ΝΑΙ |  |  |
| * Να παρίσταται στους ελέγχους που πραγματοποιεί η Ομάδα Επιθεώρησης Ελέγχου, όπως αυτή ορίζεται από την Εθνική Αρχή Κυβερνοσφάλειας, και της παρέχει όλα τα κατάλληλα μέσα για να διευκολύνει το έργο της. | ΝΑΙ |  |  |
| * Να εκτελεί ελέγχους ασφάλειας πληροφοριών και να αναφέρει τα αποτελέσματα τους στην Διοίκηση του Νοσοκομείου προκειμένου εξασφαλίζει τη συμμόρφωση του Νοσοκομείου ως προς τις υποχρεώσεις που απορρέουν από τον N. 4577/2018, την Yπουργική Aπόφαση 1027/2019 καθώς και από άλλες διατάξεις της Ευρωπαϊκής Ένωσης ή της Εθνικής Αρχής Κυβερνοασφάλειας σχετικά με την Ασφάλεια Συστημάτων Δικτύων και Πληροφοριών. | ΝΑΙ |  |  |
| * Να επιβλέπει και συντονίζει την εφαρμογή των Πολιτικών και Διαδικασιών Ασφάλειας, μέσω χρήσης κατάλληλων προτύπων, διαδικασιών και διεθνών πρακτικών και να λειτουργεί ως σημείο επαφής με τους αρμόδιους φορείς. | ΝΑΙ |  |  |
| * Να διατηρεί κατάλληλα Μέτρα και Μηχανισμούς Ασφάλειας που ικανοποιούν τις «Βασικές Απαιτήσεις Ασφαλείας», όπως αυτές ορίζονται από την Εθνική Αρχή Κυβερνοασφάλειας, για την προστασία των Πληροφοριών και Δικτύων του Νοσοκομείου. | ΝΑΙ |  |  |
| * Να φροντίζει ώστε το σύνολο των Πολιτικών και Διαδικασιών Ασφάλειας που έχουν οριστεί να είναι σε ισχύ σε όλο το εύρος του Νοσοκομείου | ΝΑΙ |  |  |
| * Να επιθεωρεί την εφαρμογή των Πολιτικών και Διαδικασιών Ασφάλειας τακτικά ή εκτάκτως σε περίπτωση που κριθεί απαραίτητο και να τις αναθεωρεί σε περίπτωση που αλλάζει κάτι ουσιαστικό στη λειτουργία του Νοσοκομείου | ΝΑΙ |  |  |
| * Να αναφέρει στην Ανώτατη Διοίκηση του Νοσοκομείου το Επίπεδο Ασφάλειας των Πληροφοριών και Δικτύων του Νοσοκομείου, το επίπεδο συμμόρφωση του με τον ν. 4577/2018 και την υπουργική απόφαση 1027/2019 καθώς και τον υπολειπόμενο κίνδυνο. | ΝΑΙ |  |  |
| * Να φέρει την ευθύνη της αξιολόγησης και διαχείρισης του εκάστοτε συμβάντος ασφαλείας και της κοινοποίησης του στην CSIRT και στην Εθνική Αρχή Κυβερνοασφάλειας. | ΝΑΙ |  |  |
| * Να επιβλέπει τους ελέγχους αποτελεσματικότητας των Μέτρων Ασφάλειας των Πολιτικών και Διαδικασιών Ασφαλείας σε όλο το εύρος του Νοσοκομείου. | ΝΑΙ |  |  |
| * Να παρακολουθεί και να συνεισφέρει στην εκτέλεση της συνεχούς παρακολούθησης της ασφάλειας των συστημάτων του Νοσοκομείου. | ΝΑΙ |  |  |
| * Να ενεργεί μέσω αναφορών ή οποιοδήποτε άλλο πρόσφορο τρόπο απέναντι στη μη συμμόρφωση με τις Πολιτικές και Διαδικασίες Ασφάλειας. | ΝΑΙ |  |  |
| * Να ενημερώνεται για τυχόν τροποποιήσεις στην ισχύουσα νομοθεσία, ώστε να εφαρμόζει τις απαραίτητες αλλαγές στις Πολιτικές Ασφάλειας. | ΝΑΙ |  |  |
| και σε κάθε περίπτωση θα πρέπει να καλύπτουν τις απαιτήσεις του ν. Ν4577/2018 καθώς και της υπουργικής απόφασης 1027/2019 καθώς και κάθε άλλη ενέργεια / στάδιο που κρίνεται απαραίτητο για την συμμόρφωση του Νοσοκομείου | ΝΑΙ |  |  |
| Ως παραδοτέα ορίζονται |  |  |  |
| * Η αποτίμηση και επικαιροποίηση των τυποποιημένων εντύπων που απαιτούνται για τη συμμόρφωση του Νοσοκομείου με τον ν. Ν4577/2018 και την υπουργική απόφαση 1027/2019 σύμφωνα με το πρότυπο ISO 27001 | ΝΑΙ |  |  |
| * Η αποτίμηση και επικαιροποίηση των Πολιτικών και Διαδικασιών Ασφάλειας Πληροφοριών και Δικτύων που καλύπτουν κατ’ ελάχιστο τον ν. 4577/2018 και την υπουργική απόφαση 1027/2019 | ΝΑΙ |  |  |
| * Η αποτίμηση και Διαχείριση της Επικινδυνότητας | ΝΑΙ |  |  |
| * Υλικό εκπαίδευσης | ΝΑΙ |  |  |
| **Προϋπολογισμός** |  |  |  |
|  |  |  |  |
| 15.000€ πλέον ΦΠΑ. | ΝΑΙ |  |  |
| **Τεχνική και Επαγγελματική Ικανότητα αναδόχου** |  |  |  |
|  |  |  |  |
| Ο ανάδοχος φορέας θα πρέπει να διαθέτει κατ’ ελάχιστον τα ακόλουθα προσόντα: |  |  |  |
|  |  |  |  |
| * Να διαθέτει πιστοποίηση κατά ISO 9001 και ISO 27001 | ΝΑΙ |  |  |
| * Η ομάδα έργου θα πρέπει να περιλαμβάνει τουλάχιστον τις ακόλουθες ειδικότητες | ΝΑΙ |  |  |
| * Information Security Consultant | ΝΑΙ |  |  |
| * IT Auditor | ΝΑΙ |  |  |
| * Νομικό Σύμβουλο | ΝΑΙ |  |  |
| * Όλα τα μέλη της ομάδας θα πρέπει να έχουν τουλάχιστον 5ετή εμπειρία σε έργα με αντικείμενο θέματα ασφάλειας πληροφοριών / προσωπικών δεδομένων | ΝΑΙ |  |  |
| * Επιπρόσθετα, ο Υπεύθυνου Ασφαλείας Πληροφοριών και Δικτύων που θα οριστεί για το Νοσοκομείο από τον οικονομικό φορέα θα αποτελεί μέρος της ομάδας έργου και θα διαθέτει τουλάχιστον: | ΝΑΙ |  |  |
| * Πιστοποίηση ISO 27001 auditor | ΝΑΙ |  |  |
| * Βεβαίωση ως Data Protection Officer (DPO) από εταιρία πιστοποιήσεων ή αντίστοιχη βεβαίωση | ΝΑΙ |  |  |
| * Πιστοποίηση Certified Information Security Manager (CISM) ή αντίστοιχη | ΝΑΙ |  |  |
| * 10ετη εμπειρία πάνω σε ασφάλεια πληροφοριών και δεδομένων | ΝΑΙ |  |  |

Ημερομηνία, ………/………./2023

(Σφραγίδα και υπογραφή νόμιμου εκπροσώπου)