Αθήνα, 25/01/2023

Αρ. πρωτ.: 2622

Τεχνικό Επιμελητήριο Ελλάδας

Σύμβαση ανάθεσης παροχής υπηρεσιών σχετικά με το σύστημα διαχείρισης δαπανών του ΤΕΕ ποσού είκοσι εννέα χιλιάδων εννιακοσίων ευρώ (29.900,00€) πλέον Φ.Π.Α

Στην Αθήνα σήμερα, 25/01/2023, στα γραφεία του Τεχνικού Επιμελητηρίου Ελλάδας (Κεντρική Υπηρεσία), επί της οδού Νίκης 4, Τ.Κ 105 63, μεταξύ των κατωτέρω συμβαλλομένων, ήτοι:

α) ***Αφενός μεν*** του Νομικού Πρόσωπου Δημοσίου Δικαίου (‘ΝΠΔΔ’) με την επωνυμία «**Τεχνικό Επιμελητήριο Ελλάδας**», που εδρεύει στον Δήμο Αθηναίων επί της οδού Νίκης, αρ. 4, Τ.Κ. 105 63, με Α.Φ.Μ. 090002260, υπαγόμενο στη ΔΟΥ Δ΄ Αθηνών, και εκπροσωπείται νόμιμα από τον Πρόεδρο, κ. **Γιώργο Ν. Στασινό**, αναφερόμενο εφ’ εξής ως «**Τ.Ε.Ε.**»,

β) ***Αφετέρου δε*** της εταιρίας με την επωνυμία **«NEUROPUBLIC Ανώνυμη Εταιρεία Πληροφορικής και Επικοινωνιών»** και το διακριτικό τίτλο **«NEUROPUBLIC ΑΕ»** που εδρεύει στον Πειραιά,επί της οδού Μεθώνης 6, Τ.Κ 18545, με ΑΦΜ 999608870**,** υπαγόμενη στη ΔΟΥ ΦΑΕ ΠΕΙΡΑΙΑ και εκπροσωπείται νομίμως από την κα **Ρόζα Γαργαλάκου** του **Αναστασίου**, αναφερόμενης στο εξής ως «**Ανάδοχος**»,

αφού ελήφθησαν υπόψη

- Ο νόμος 4412/2016 (ΦΕΚ Α 147/ 08.08.2016) «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών» όπως ισχύει,
- Ο νόμος 4782/2021(ΦΕΚ Α’36-09/03/2021) «Εκσυγχρονισμός, απλοποίηση και αναμόρφωση του ρυθμιστικού πλαισίου των δημοσίων συμβάσεων, ειδικότερες ρυθμίσεις προμηθειών στους τομείς της άμυνας και της ασφάλειας και άλλες διατάξεις για την ανάπτυξη, τις υποδομές και την υγεία», όπως ισχύει,
- Ο Κανονισμός (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 για την Προστασία Δεδομένων) εφεξής Κανονισμός,
- Ο νόμος 4624/2019 ως προς τα μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την

προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και στην ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις,

- Η υπ' αριθ. **Α51/Σ41/2022** (ΑΔΑ:9ΨΑΚ46Ψ842-1Τ5) απόφαση της Διοικούσας Επιτροπής του ΤΕΕ, δυνάμει της οποίας αποφασίστηκε η έγκριση σκοπιμότηταςκαι Ανάθεση για την προμήθεια συμβουλευτικών υπηρεσιών σχετικά με το «σύστημα διαχείρισης δαπανών του ΤΕΕ»,
- Η με αρ. πρωτ. **ΔΟΥ/995 / 22.11.2022** Απόφαση Ανάληψης Υποχρέωσης (ΑΔΑ:67ΙΗ46Ψ842-ΨΞΚ),
- Η με αρ. πρωτ. **32636/22.11.2022** Πρόσκληση Εκδήλωσης Ενδιαφέροντος που αφορά την παροχή υπηρεσιών σχετικά με το σύστημα διαχείρισης δαπανών του ΤΕΕ,
- Η προσφορά της Αναδόχου (αρ. Πρωτ. ΤΕΕ : **33014/25.11.2022**),

συμφωνήθηκαν, συνομολογήθηκαν και έγιναν αμοιβαία αποδεκτά τα εξής :

ΑΡΘΡΟ 1

ΑΝΤΙΚΕΙΜΕΝΟ-ΠΑΡΑΔΟΤΕΑ

Αντικείμενο της Σύμβασης αποτελεί η παροχή υπηρεσιών σχετικά με το σύστημα διαχείρισης δαπανών του ΤΕΕ. Πιο συγκεκριμένα, οι υπηρεσίες που θα παρασχεθούν από τον ανάδοχο προς το ΤΕΕ, αφορούν σε γενική περιγραφή τα ακόλουθα:

1. Αρχιτεκτονική του συστήματος

Το σύστημα πρέπει να βασίζεται σε 3-tier αρχιτεκτονική (rdbms, webserver, web-browser) και από την πλευρά του τελικού χρήστη να μην απαιτείται επιπλέον εγκατάσταση λογισμικού. Να υποστηρίζονται οι πιο δημοφιλείς browser για περιβάλλον Microsoft Windows. Η εγκατάσταση του συστήματος να δύναται να υλοποιηθεί είτε σε εγκαταστάσεις ΤΕΕ (VM) είτε σε κυβερνητικό cloud. Θα πρέπει να υποστηρίζεται η λειτουργία ανεξάρτητων (σε επίπεδο προϋπολογισμού) τμημάτων του ΤΕΕ.

2. Επίπεδα ασφαλείας

Το σύστημα πρέπει να έχει την δυνατότητα απεριόριστων χρηστών, και την δυνατότητα διαχωρισμού επιπέδων πρόσβασης σε κάθε διακριτή λειτουργία (θέαση, εισαγωγή, ενημέρωση, διαγραφή, έγκριση).

3. Διαχείριση Συμβάσεων

Η διαχείριση των συμβάσεων από το σύστημα πρέπει να καλύπτει την αρχική απόφαση, δέσμευση ποσών, ροή ανάθεσης και τελική σύμβαση (με τυχόν αναθεωρήσεις) με πολλαπλούς δικαιούχους.

4. Παρακολούθηση Συμβάσεων

Το σύστημα πρέπει να παρέχει τη δυνατότητα παρακολούθησης των υπογεγραμμένων συμβάσεων, βάσει των προβλεπόμενων ημερομηνιών, των Εγκρίσεων Καταβολής της Διοικούσας Επιτροπής καθώς και των λοιπών στοιχείων της σύμβασης.

5. Προϋπολογισμός-Γενική Λογιστική

Το σύστημα θα πρέπει να παρέχει επιπλέον τη δυνατότητα εισαγωγής Προϋπολογισμού (ΚΑΕ) με δυνατότητα πολλαπλών επιπέδων λογαριασμών, τροποποιήσεις και παρακολούθηση δεσμεύσεων, αποδεσμεύσεων, πραγματικής εκτέλεσης (σύμβαση, ένταλμα, πληρωμή κλπ), μεταφοράς σε νέα χρήση, πολυετείς δεσμεύσεις κλπ.

6. Καταχώρηση παραστατικών - Έκδοση Ενταλμάτων

Σε κάθε εγκεκριμένη δαπάνη να δύναται να εκδοθεί έγκριση καταβολής, ένταλμα πληρωμής καθώς και αντίστοιχου παραστατικού (όπου απαιτείται) με αυτοματισμό κρατήσεων ή την καταχώρηση κρατήσεων ad-hoc όπου απαιτείται. Επίσης είναι επιθυμητό να δύναται εξουσιοδοτημένος χρήστης του ΤΕΕ να ενημερώνει ή να δημιουργεί νέα πρότυπα κρατήσεων.

7. Εκτέλεση-Εκκαθάριση Δαπανών

Το σύστημα θα πρέπει να υποστηρίζει τη πληρωμή με απευθείας διασύνδεση ή εξαγωγή αρχείου ανάλογα με τις συνεργαζόμενες Τράπεζες. Σε αρχική λειτουργία πρέπει να υποστηριχθεί η πληρωμή μέσω ΕΤΕ και προαιρετικά μέσω ΔΙΑΣ. Τέλος, θα πρέπει να υπάρχει η δυνατότητα απόδοσης κρατήσεων ανά κατηγορία και περιοδικότητα.

8. Παρακολούθηση πληρωμών

Θα πρέπει επιπλέον το σύστημα να υποστηρίζει την ανάρτηση αρχείων στην Ε.Α.Π.

9. Αναφορές

Το σύστημα πρέπει να παρέχει τις απαραίτητες αναφορές για την έκδοση εγγράφων και την παρακολούθηση συμβάσεων, προϋπολογισμού, δαπανών κλπ με πολλαπλά φίλτρα αναζήτησης. Επιπλέον πρέπει με εύκολο τρόπο να δημιουργούνται επιπλέον αναφορές σύμφωνα με τις απαιτήσεις του ΤΕΕ. Να υπάρχει η δυνατότητα αλλαγής σταθερών σημείων (πχ ονόματα υπευθύνων κλπ) από τον τελικό χρήστη. Έκδοση βεβαιώσεων αποδοχών με το σύνολο των αποδοχών μισθοδοσίας και πρόσθετων αμοιβών πχ ομάδες εργασίας με διασύνδεση με την μισθοδοσία σε επίπεδο ΑΦΜ ή και άλλων κριτηρίων.

10. Βοηθητικές Λειτουργίες

Στις βοηθητικές λειτουργίες πρέπει να παρέχεται η δυνατότητα (μέσω γνωστής δομής αρχείων) για τη μαζική καταχώρηση παραστατικών και ενταλμάτων από προγράμματα τρίτων που χρησιμοποιεί το ΤΕΕ.

11. Διασυνδέσεις

Θα πρέπει το σύστημα να παρέχει διασύνδεση με πύλες υποχρεωτικής ανάρτησης (όπου αυτές διατίθενται) όπως ΔΙΑΥΓΕΙΑ, ΕΣΗΔΗΣ, ΚΗΜΔΗΣ, e-ΠΔΕ, TAXISnet (διάφορα επίπεδα), ΕΑΠ, MyΑΑΔΕ κλπ.

12. Αποθήκευση Αδόμητης Πληροφορίας

Σε κάθε κομβικό σημείο (συμβάσεις, πρωτόκολλα παραλαβής, παραστατικά, δικαιολογητικά) θα πρέπει να παρέχεται η δυνατότητα αποθήκευσης ψηφιοποιημένων αρχείων.

ΑΡΘΡΟ 2

ΔΙΑΡΚΕΙΑ- ΠΟΙΟΤΙΚΗ – ΠΟΣΟΤΙΚΗ ΠΑΡΑΛΑΒΗ

Η σύμβαση θα έχει διάρκεια **δύο (2) μήνες από την υπογραφή της σύμβασης**.

Η πιστοποίηση της παροχής των παραπάνω υπηρεσιών από τον Ανάδοχο στο ΤΕΕ θα γίνει από την αρμόδια Επιτροπή Παραλαβής του ΤΕΕ, όπως αυτή ορίστηκε με την υπ' αρ. Α18/Σ43/2022 (ΑΔΑ:9Ρ6Ο46Ψ842-Ξ5Ε), απόφαση της ΔΕ του ΤΕΕ για το έτος 2023 και όπως αυτή θα τροποποιηθεί στο μέλλον, η οποία θα βεβαιώνει την καλή εκτέλεση.

Οι Υπεύθυνοι Παραλαβής θα ελέγξουν αν η Ανάδοχος εκτέλεσε τους όρους της παρούσας σύμβασης και θα προβούν εγγράφως σε συστάσεις και υποδείξεις σε αυτήν εφόσον διαπιστωθεί απόκλιση. Η Ανάδοχος υποχρεούται να συμμορφωθεί εγκαίρως και προσηκόντως προς τις ανωτέρω υποδείξεις και συστάσεις εφόσον προκύψουν.

ΑΡΘΡΟ 3

ΑΜΟΙΒΗ - ΤΡΟΠΟΣ ΠΛΗΡΩΜΗΣ – ΚΡΑΤΗΣΕΙΣ – ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ

Η συνολική δαπάνη θα ανέλθει στο ποσό των**είκοσι εννέα χιλιάδων εννιακοσίων ευρώ (29.900,00 €)** πλέον του αναλογούντος **Φ.Π.Α. 24%** ποσού **επτά χιλιάδων εκατόν εβδομήντα έξι ευρώ (7.176,00 €)** ήτοι στο συνολικό ποσό των **τριάντα επτά χιλιάδων εβδομήντα έξι ευρώ** (**37.076,00 €**) στο οποίο περιλαμβάνονται όλες οι τυχόν επιβαρύνσεις. Η πληρωμή της «Αναδόχου» θα γίνεται μετά την πιστοποίηση της παραλαβής των παραδοτέων από την αρμόδια Επιτροπή Παραλαβής του ΤΕΕ, και την έκδοση χρηματικού εντάλματος πληρωμής. Η δαπάνη θα βαρύνει τον **ΚΑ 9761.01.**

Η «Ανάδοχος» υποχρεούται στην έκδοση τιμολογίου, επί του οποίου θα γίνονται οι νόμιμες κρατήσεις και η παρακράτηση φόρου. **Απαραίτητα δικαιολογητικά για την εξόφληση του τιμολογίου είναι η προσκόμιση προσήκουσας φορολογικής και ασφαλιστικής ενημερότητας.** Οποιαδήποτε έξοδα (όλως ενδεικτικά: χαρτόσημα, νόμιμες κρατήσεις κ.λπ.) βαρύνουν την «Ανάδοχο».

ΑΡΘΡΟ 4

ΔΙΚΑΙΩΜΑΤΑ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

Η Ανάδοχος υποχρεούται να μην προβεί σε καμία απολύτως πράξη προσβολής των δικαιωμάτων πνευματικής ιδιοκτησίας του ΤΕΕ, καθώς και των δεδομένων προσωπικού χαρακτήρα των μελών ή συνεργατών αυτού, που τυχόν έρθουν εις γνώση της, καθ΄ οιονδήποτε τρόπο, ενώ ταυτόχρονα οφείλει να ενημερώσει το ΤΕΕ, για οποιαδήποτε περίπτωση προσβολής αυτών υποπέσει στην αντίληψή της.

ΑΡΘΡΟ 5

ΡΗΤΡΑ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ – ΕΧΕΜΥΘΕΙΑΣ

Καθ΄ όλη τη διάρκεια της σύμβασης αλλά και μετά τη λήξη ή λύση αυτής, η Ανάδοχος υποχρεούται να τηρήσει εμπιστευτικές και να μην γνωστοποιήσει σε οποιονδήποτε τρίτο, οποιαδήποτε έγγραφα ή πληροφορίες που θα περιέλθουν εις γνώση του κατά την υλοποίηση της σύμβασης και την εκπλήρωση των υποχρεώσεων του. Επίσης υποχρεούται να μην γνωστοποιήσει μέρος ή το σύνολο της σύμβασης που θα εκτελέσει χωρίς την προηγούμενη έγγραφη άδεια του ΤΕΕ.

Η Ανάδοχος υποχρεούται να διασφαλίσει ασφαλές πληροφορικό περιβάλλον ώστε ουδείς τρίτος προς το ΤΕΕ -υπερκείμενος ή υποκείμενος - αυτού να μπορεί να έχει πρόσβαση στο δίκτυο πληροφοριών του χωρίς την προηγούμενη δική της έγκριση.

Η Ανάδοχος υποχρεούται να τηρεί εχεμύθεια ως προς τις εμπιστευτικές πληροφορίες και τα στοιχεία που σχετίζονται με τις δραστηριότητες του ΤΕΕ. Ως εμπιστευτικές πληροφορίες και στοιχεία νοούνται όσα δεν είναι γνωστά στους τρίτους, ακόμα και αν δεν έχουν χαρακτηρισθεί από το ΤΕΕ ως εμπιστευτικά. Η τήρηση εμπιστευτικών πληροφοριών από το Συνεργάτη διέπεται από τις κείμενες διατάξεις και το νομοθετικό πλαίσιο και πρέπει να είναι εφάμιλλη της εμπιστευτικότητας που τηρεί η Ανάδοχος για τον ίδιο και για τις δικές τους πληροφορίες εμπιστευτικού χαρακτήρα.

Η Ανάδοχος υποχρεούται να αποφεύγει οποιαδήποτε εμπλοκή των συμφερόντων του με τα συμφέροντα του ΤΕΕ, να παραδώσει με τη λήξη της Σύμβασης όλα τα στοιχεία, έγγραφα κλπ. που έχει στην κατοχή του και αφορούν στο ΤΕΕ ή/και το Ελληνικό Δημόσιο και να τηρεί μια πλήρη σειρά των αρχείων και εγγράφων και του λοιπού υλικού που αφορά στην υλοποίηση των παρεχόμενων υπηρεσιών. Τα αρχεία αυτά πρέπει να είναι εύκολα διαχωρίσιμα από άλλα αρχεία του Συνεργάτη που δεν αφορούν το Έργο.

Η Ανάδοχος υποχρεούται να προστατεύει το απόρρητο και τα αρχεία που αφορούν σε προσωπικά δεδομένα ατόμων και που τυχόν έχει στην κατοχή του για την υλοποίηση

της σύμβασης, ακόμη και μετά την ολοκλήρωση των παρεχόμενων υπηρεσιών, να επιτρέπει στο ΤΕΕ και στα άτομα που ορίζονται από αυτό να διενεργούν, κατόπιν έγγραφης αιτήσεως, ελέγχους των τηρούμενων αρχείων προκειμένου να αξιολογηθεί η δυνατότητα υλοποίησης και ολοκλήρωσης της σύμβασης με βάση τα αναφερόμενα σ αυτήν.

Η Ανάδοχος οφείλει να λάβει όλα τα αναγκαία μέτρα προκειμένου να διασφαλίσει ότι και οι εργαζόμενοι/συνεργάτες/υπεργολάβοι του γνωρίζουν και συμμορφώνονται με τις παραπάνω υποχρεώσεις. Τα συμβαλλόμενα μέρη συμφωνούν ότι σε περίπτωση υπαιτιότητας του Συνεργάτη στη μη τήρηση των παραπάνω υποχρεώσεων εχεμύθειας, η Ανάδοχος θα καταβάλλει στο ΤΕΕ ποινική ρήτρα ίση με το ποσό της αμοιβής του από τη Σύμβαση. Επίσης, το ΤΕΕ διατηρεί το δικαίωμα να απαιτήσει από το Συνεργάτη την αποκατάσταση κάθε τυχόν περαιτέρω ζημίας.

Η Ανάδοχος αναλαμβάνει την υποχρέωση να τηρήσει ως άκρως εμπιστευτικά και να μη γνωστοποιήσει σε οποιοδήποτε τρίτο οποιαδήποτε δεδομένα, έγγραφα ή πληροφορίες που θα περιέλθουν σε γνώση της κατά την εκπλήρωση των υποχρεώσεών του. Η Ανάδοχος υποχρεούται να λάβει όλα τα αναγκαία μέτρα προκειμένου να εξασφαλίσει ότι το σύνολο των εργαζομένων της γνωρίζουν και συμμορφώνονται προς τις υποχρεώσεις που προκύπτουν από το παρόν άρθρο και παράλληλα να εξασφαλίσει την διαφύλαξη και ασφάλεια των ανωτέρω πληροφοριών και στοιχείων και την παρεμπόδιση πρόσβασης μη εξουσιοδοτημένων τρίτων σε αυτά.

Το ΤΕΕ δεσμεύεται να τηρεί εμπιστευτικά για δύο (2) έτη τα στοιχεία που τίθενται στη διάθεσή του από την Ανάδοχο εάν αφορούν σε τεχνικά στοιχεία ή πληροφορίες και τεχνογνωσία ή δικαιώματα πνευματικής ιδιοκτησίας εφόσον αυτά φέρουν την ένδειξη «εμπιστευτικό έγγραφο». Σε καμία περίπτωση η εμπιστευτικότητα δεν δεσμεύει το ΤΕΕ προς τις αρχές του Ελληνικού Κράτους και της Ευρωπαϊκής Ένωσης.

Η εμπιστευτικότητα αίρεται αυτοδικαίως σε περίπτωση εκκρεμούς δίκης, ένστασης, διαιτησίας, στο απολύτως αναγκαίο μέτρο και αποκλειστικά για χρήση της από τα μέρη, τους δικαστικούς παραστάτες καθώς και τους δικαστές της διαιτησίας.

ΑΡΘΡΟ 6

ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Τα μέρη συμφωνούν ότι θα συλλέγουν και εν γένει θα επεξεργάζονται πληροφορίες που συνιστούν προσωπικά δεδομένα σύμφωνα με το ενωσιακό και εθνικό ρυθμιστικό πλαίσιο περί προστασίας προσωπικών δεδομένων και συγκεκριμένα το Κανονισμό (ΕΕ) 2016/679 (Γενικός Κανονισμός Προστασίας Δεδομένων), τη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης, τον Εθνικό νόμο 4624/2019, καθώς και τις πράξεις

(Αποφάσεις, Οδηγίες και Γνωμοδοτήσεις) του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων και της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) . Η συμβατική σχέση των μερών ως προς την επεξεργασία των προσωπικών δεδομένων, ρυθμίζεται στο Παράρτημα Επεξεργασίας Δεδομένων, το οποίο αποτελεί αναπόσπαστο τμήμα της παρούσας Σύμβασης.

ΑΡΘΡΟ 7

ΠΑΡΑΒΑΣΕΙΣ – ΠΟΙΝΙΚΕΣ ΡΗΤΡΕΣ

Σε περίπτωση μη εκτέλεσης ή μη προσήκουσας ή μη έγκαιρης εκτέλεσης των όρων της παρούσας σύμβασης, οι οποίοι θεωρούνται όλοι ουσιώδεις, και οφείλονται αποδεδειγμένα στην Ανάδοχο, η Ανάδοχος δύναται να κηρυχθεί έκπτωτος, αφού προηγουμένως αποτύχουν οι ενέργειες φιλικής διευθέτησης, με Απόφαση της ΔΕ του ΤΕΕ. Στην περίπτωση αυτή το ΤΕΕ διατηρεί το δικαίωμα να αξιώσει από την Ανάδοχο την καταβολή αποζημίωσης για οποιαδήποτε αποδεδειγμένη ζημία, άμεση ή έμμεση, υποστεί.

Σε περίπτωση αποδεδειγμένης ευθύνης της Αναδόχου στην καθυστέρηση της παροχής των παραπάνω υπηρεσιών και εν γένει πλημμελούς εκπλήρωσης των αναλαμβανομένων υποχρεώσεων και αφού προηγουμένως αποτύχουν οι ενέργειες φιλικής διευθέτησης των ενδεχόμενων διαφορών, η Ανάδοχος υποχρεούται στην καταβολή προς το ΤΕΕ του ποσού των **εκατόν πενήντα ευρώ (150,00€)** για κάθε ημέρα καθυστέρησης, ως ποινική ρήτρα, η οποία συμφωνείται από τούδε εύλογη, δίκαιη, σύμφωνη με τα χρηστά συναλλακτικά ήθη και ανάλογη με το σκοπό για τον οποίο συμφωνείται. Το προαναφερόμενο ποσό της ποινικής ρήτρας θα καταβάλλεται ανεξάρτητα από την ως άνω αποζημίωση.

ΑΡΘΡΟ 8

ΥΠΕΡΓΟΛΑΒΙΑ – ΕΚΧΩΡΗΣΗ

Ρητώς συμφωνείται ότι η Ανάδοχος δεν έχει δικαίωμα να εκχωρήσει το σύνολο ή μέρος των υποχρεώσεων ή των απαιτήσεών του που απορρέουν από την παρούσα σε τρίτο χωρίς την έγγραφη σχετική συναίνεση του ΤΕΕ, άλλως κηρύσσεται έκπτωτος.

ΑΡΘΡΟ 9

ΙΣΧΥΟΝ ΔΙΚΑΙΟ

Η παρούσα σύμβαση διέπεται από το ελληνικό δίκαιο. Για όλα τα λοιπά θέματα της παρούσας ισχύουν οι κείμενες διατάξεις που ρυθμίζουν τους όρους και προϋποθέσεις περί ανάληψης υποχρεώσεων και περί προμηθειών του Δημοσίου και ιδίως του Ν.

4412/2016 (ΦΕΚ Α 147/ 08.08.2016) «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών» και του Ν. 2690/99 (ΦΕΚ 45 Α΄/99) «Περί κύρωσης του Κώδικα Διοικητικής Διαδικασίας και άλλες διατάξεις», όπως ισχύουν.

ΑΡΘΡΟ 10

ΔΙΚΑΣΤΙΚΗ ΕΠΙΛΥΣΗ ΔΙΑΦΟΡΩΝ – ΔΩΣΙΔΙΚΙΑ – ΕΦΑΡΜΟΣΤΕΟ ΔΙΚΑΙΟ – ΤΡΟΠΟΠΟΙΗΣΕΙΣ & ΣΥΜΠΛΗΡΩΣΕΙΣ

Για κάθε διαφορά που απορρέει αμέσως ή εμμέσως από τη σύμβαση αυτή και αφορά την ερμηνεία ή/και την εκτέλεσή της αρμόδια είναι αποκλειστικά τα δικαστήρια των Αθηνών και εφαρμοστέο δίκαιο το ελληνικό.

Τυχόν ακυρότητα όρου/όρων της παρούσας δεν επηρεάζει το κύρος των υπολοίπων όρων, τα δε συμβαλλόμενα μέρη υποχρεούνται να καλύψουν το κενό που ενδέχεται να προκύψει εξαιτίας ακυρότητας όρου/όρων ερμηνευτικά ή και με συμπλήρωση της παρούσας κατά τρόπο που να εκπληρούται ο οικονομικός σκοπός της.

Οποιαδήποτε τροποποίηση ή και συμπλήρωση της παρούσας σύμβασης πραγματοποιείται και είναι ισχυρή μόνον εφόσον γίνει εγγράφως και προσυπογραφεί νομίμως και από τα δύο συμβαλλόμενα μέρη, αποδεικνύεται δε μόνον εγγράφως, αποκλειομένου οιουδήποτε άλλου αποδεικτικού μέσου.

Σε πίστωση των ανωτέρω συντάχθηκε η παρούσα σύμβαση, η οποία αφού διαβάστηκε και βεβαιώθηκε για το περιεχόμενό της, υπογράφηκε, νόμιμα και ως έπεται, από τους συμβαλλόμενους, σε τρία (3) όμοια και ισόκυρα πρωτότυπα, εκ των οποίων (2) έλαβε το ΤΕΕ και ένα (1) η Ανάδοχος για κάθε νόμιμη χρήση.

ΤΑ ΣΥΜΒΑΛΛΟΜΕΝΑ ΜΕΡΗ

Για το ΤΕΕ	Για την Ανάδοχο
Ο Πρόεδρος	Η Νόμιμη Εκπρόσωπος
Γιώργος Ν. Στασινός	Ρόζα Γαργαλάκου

Συνημμένα :

- ΠΑΡΑΡΤΗΜΑ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
- ΠΡΟΣΑΡΤΗΜΑ 1
- ΠΡΟΣΑΡΤΗΜΑ 2

ΠΑΡΑΡΤΗΜΑ

Τυποποιημένες συμβατικές ρήτρες

ΤΜΗΜΑ Ι

Ρήτρα 1

Σκοπός και πεδίο εφαρμογής

α) Οι παρούσες τυποποιημένες συμβατικές ρήτρες (στο εξής: ρήτρες) έχουν ως σκοπό να διασφαλίζουν τη συμμόρφωση με το άρθρο 28 παράγραφοι 3 και 4 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).

β) Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία που απαριθμούνται στο προσάρτημα Ι συμφώνησαν τις παρούσες ρήτρες προκειμένου να διασφαλίζεται η συμμόρφωση με το άρθρο 28 παράγραφοι 3 και 4 του κανονισμού (ΕΕ) 2016/679.

γ) Οι παρούσες ρήτρες εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα όπως καθορίζεται στο προσάρτημα ΙΙ.

δ) Τα προσαρτήματα Ι έως IV είναι αναπόσπαστο μέρος των ρητρών.

ε) Οι παρούσες ρήτρες δεν θίγουν τις υποχρεώσεις στις οποίες υπόκειται ο υπεύθυνος επεξεργασίας δυνάμει του κανονισμού (ΕΕ) 2016/679.

στ) Οι παρούσες ρήτρες δεν διασφαλίζουν από μόνες τους τη συμμόρφωση με τις υποχρεώσεις που σχετίζονται με τις διεθνείς διαβιβάσεις σύμφωνα με το κεφάλαιο V του κανονισμού (ΕΕ) 2016/679.

Ρήτρα 2

Αμετάβλητος χαρακτήρας των ρητρών

α) Τα μέρη δεσμεύονται να μην τροποποιούν τις ρήτρες παρά μόνο για να προσθέσουν ή να επικαιροποιήσουν πληροφορίες στα προσαρτήματα.

β) Η δέσμευση αυτή δεν εμποδίζει τα μέρη να ενσωματώνουν τις τυποποιημένες συμβατικές ρήτρες που ορίζονται στις παρούσες ρήτρες σε ευρύτερη σύμβαση ούτε να προσθέτουν άλλες ρήτρες ή πρόσθετες εγγυήσεις, υπό τον όρο ότι αυτές δεν αντιφάσκουν, άμεσα ή έμμεσα, προς τις ρήτρες ούτε θίγουν τα θεμελιώδη δικαιώματα ή τις ελευθερίες των υποκειμένων των δεδομένων.

Ρήτρα 3

Ερμηνεία

α) Όπου στις παρούσες ρήτρες χρησιμοποιούνται όροι που ορίζονται στον κανονισμό (ΕΕ) 2016/679, οι εν λόγω όροι έχουν την ίδια έννοια με αυτή που έχουν στον οικείο κανονισμό.

β) Η ανάγνωση και ερμηνεία των παρουσών ρητρών πραγματοποιούνται υπό το πρίσμα των διατάξεων του κανονισμού (ΕΕ) 2016/679.

γ) Οι παρούσες ρήτρες δεν ερμηνεύονται με τρόπο που αντιβαίνει προς τα δικαιώματα και τις υποχρεώσεις που προβλέπονται στον κανονισμό (ΕΕ) 2016/679 ή με τρόπο που θίγει τα θεμελιώδη δικαιώματα ή τις ελευθερίες των υποκειμένων των δεδομένων.

Ρήτρα 4

Ιεραρχία

Σε περίπτωση αντίφασης μεταξύ των παρουσών ρητρών και των διατάξεων συναφών συμφωνιών μεταξύ των μερών οι οποίες ισχύουν κατά τον χρόνο που συμφωνούνται ή συνάπτονται οι παρούσες ρήτρες, οι παρούσες ρήτρες υπερισχύουν.

ΤΜΗΜΑ ΙΙ

ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΣΥΜΒΑΛΛΟΜΕΝΩΝ ΜΕΡΩΝ

Ρήτρα 5

Περιγραφή της επεξεργασίας

Οι λεπτομέρειες των πράξεων επεξεργασίας, ιδίως οι κατηγορίες των δεδομένων προσωπικού χαρακτήρα και οι σκοποί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας, καθορίζονται στο προσάρτημα ΙΙ.

Ρήτρα 6

Υποχρεώσεις των συμβαλλόμενων μερών

6.1. Εντολές

α) Ο εκτελών την επεξεργασία επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο βάσει του δικαίου της Ένωσης ή του δικαίου του κράτους μέλους στο οποίο υπόκειται ο εκτελών την επεξεργασία. Στην περίπτωση αυτή, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας για την εν λόγω νομική απαίτηση πριν από την επεξεργασία, εκτός εάν το εν λόγω δίκαιο απαγορεύει αυτού του είδους την ενημέρωση για σοβαρούς λόγους δημόσιου συμφέροντος. Ο υπεύθυνος επεξεργασίας μπορεί επίσης να δίνει μεταγενέστερες εντολές καθ' όλη τη διάρκεια της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Οι εν λόγω εντολές είναι πάντοτε έγγραφες.

β) Ο εκτελών την επεξεργασία ενημερώνει αμέσως τον υπεύθυνο επεξεργασίας, εάν, κατά την άποψη του εκτελούντος της επεξεργασία, κάποια εντολή του υπευθύνου επεξεργασίας παραβιάζει τον κανονισμό (ΕΕ) 2016/679 ή ενωσιακές ή εθνικές διατάξεις περί προστασίας δεδομένων.

6.2. Περιορισμός του σκοπού

Ο εκτελών την επεξεργασία επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο για τον συγκεκριμένο σκοπό ή σκοπούς της επεξεργασίας που ορίζονται στο προσάρτημα ΙΙ, εκτός αν λάβει περαιτέρω εντολές από τον υπεύθυνο επεξεργασίας.

6.3. Διάρκεια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα

Η επεξεργασία από τον εκτελούντα την επεξεργασία πραγματοποιείται μόνο για το χρονικό διάστημα που καθορίζεται στο προσάρτημα ΙΙ.

6.4. Ασφάλεια της επεξεργασίας

α) Ο εκτελών την επεξεργασία εφαρμόζει τουλάχιστον τα τεχνικά και οργανωτικά μέτρα που καθορίζονται στο προσάρτημα ΙΙΙ προκειμένου να διασφαλίζει την ασφάλεια των δεδομένων προσωπικού χαρακτήρα. Στο πλαίσιο αυτό συμπεριλαμβάνεται η προστασία των δεδομένων από παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων

(στο εξής: παραβίαση δεδομένων προσωπικού χαρακτήρα). Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, τα συμβαλλόμενα μέρη λαμβάνουν δεόντως υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής, τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους που συντρέχουν για τα υποκείμενα των δεδομένων.

β) Ο εκτελών την επεξεργασία παρέχει σε μέλη του προσωπικού του πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία μόνο στο μέτρο που είναι απολύτως αναγκαίο για την εκτέλεση, τη διαχείριση και την παρακολούθηση της σύμβασης. Ο εκτελών την επεξεργασία διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα λαμβανόμενα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή υπόκεινται σε δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας.

6.5. Ευαίσθητα δεδομένα

Αν η επεξεργασία περιλαμβάνει δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, γενετικά δεδομένα ή βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία ή τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό φυσικού προσώπου, ή δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα (στο εξής: ευαίσθητα δεδομένα), ο εκτελών την επεξεργασία εφαρμόζει ειδικούς περιορισμούς και/ή πρόσθετες εγγυήσεις.

6.6. Τεκμηρίωση και συμμόρφωση

α) Τα συμβαλλόμενα μέρη είναι σε θέση να αποδείξουν τη συμμόρφωσή τους με τις παρούσες ρήτρες.

β) Ο εκτελών την επεξεργασία ανταποκρίνεται άμεσα και επαρκώς σε όλα τα αιτήματα πληροφοριών του υπευθύνου επεξεργασίας σχετικά με την επεξεργασία δεδομένων σύμφωνα με τις παρούσες ρήτρες.

γ) Ο εκτελών την επεξεργασία θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης προς τις υποχρεώσεις που καθορίζονται στις παρούσες ρήτρες και απορρέουν απευθείας από τον κανονισμό (ΕΕ) 2016/679. Επιπλέον, κατόπιν αιτήματος του υπευθύνου επεξεργασίας, ο εκτελών την επεξεργασία επιτρέπει και διευκολύνει ελέγχους των δραστηριοτήτων επεξεργασίας που καλύπτονται από τις παρούσες ρήτρες, σε εύλογα τακτά χρονικά διαστήματα ή αν υπάρχουν ενδείξεις μη συμμόρφωσης. Όταν αποφασίζει για επανεξέταση ή έλεγχο, ο υπεύθυνος επεξεργασίας μπορεί να λαμβάνει υπόψη σχετικές πιστοποιήσεις του εκτελούντος την επεξεργασία.

δ) Ο υπεύθυνος επεξεργασίας μπορεί να επιλέγει να διενεργήσει τον έλεγχο ο ίδιος ή να τον αναθέσει σε ανεξάρτητο ελεγκτή. Οι έλεγχοι είναι δυνατόν να περιλαμβάνουν και επιθεωρήσεις στους χώρους ή τις φυσικές εγκαταστάσεις του εκτελούντος την επεξεργασία, ενώ, όταν ενδείκνυται, διενεργούνται έπειτα από εύλογη προθεσμία προειδοποίησης.

ε) Τα συμβαλλόμενα μέρη θέτουν τις πληροφορίες που αναφέρονται στην παρούσα ρήτρα, συμπεριλαμβανομένων των αποτελεσμάτων τυχόν ελέγχων, στη διάθεση της αρμόδιας εποπτικής αρχής (ΑΠΔΠΧ), κατόπιν σχετικού αιτήματός της.

6.7. Χρήση υπεργολάβων επεξεργασίας

α) Ο εκτελών την επεξεργασία δεν αναθέτει σε υπεργολάβο επεξεργασίας καμία από τις πράξεις επεξεργασίας που εκτελεί για λογαριασμό του υπευθύνου επεξεργασίας σύμφωνα με τις παρούσες ρήτρες, χωρίς την προηγούμενη ειδική γραπτή άδεια του υπευθύνου επεξεργασίας.
β) Όταν ο εκτελών την επεξεργασία προσλαμβάνει υπεργολάβο επεξεργασίας για την εκτέλεση συγκεκριμένων δραστηριοτήτων επεξεργασίας (για λογαριασμό του υπευθύνου επεξεργασίας), το πράττει μέσω σύμβασης η οποία επιβάλλει στον υπεργολάβο επεξεργασίας, στην ουσία, τις ίδιες υποχρεώσεις όσον αφορά την προστασία των δεδομένων με αυτές που επιβάλλονται στον εκτελούντα την επεξεργασία σύμφωνα με τις παρούσες ρήτρες. Ο εκτελών την επεξεργασία διασφαλίζει ότι ο υπεργολάβος επεξεργασίας συμμορφώνεται με τις υποχρεώσεις στις οποίες υπόκειται ο εκτελών την επεξεργασία σύμφωνα με τις παρούσες ρήτρες και τον κανονισμό (ΕΕ) 2016/679.
γ) Κατόπιν αιτήματος του υπευθύνου επεξεργασίας, ο εκτελών την επεξεργασία παρέχει στον υπεύθυνο επεξεργασίας αντίγραφο της συμφωνίας με τον υπεργολάβο και κάθε τυχόν μεταγενέστερης πράξης τροποποίησής της. Στον βαθμό που είναι αναγκαίο για την προστασία επαγγελματικών απορρήτων ή άλλων εμπιστευτικών πληροφοριών, συμπεριλαμβανομένων των δεδομένων προσωπικού χαρακτήρα, ο εκτελών την επεξεργασία μπορεί να απαλείψει τις εμπιστευτικές πληροφορίες από το κείμενο της συμφωνίας πριν από την κοινοποίηση του αντιγράφου.
δ) Ο εκτελών την επεξεργασία παραμένει πλήρως υπεύθυνος έναντι του υπευθύνου επεξεργασίας για την εκπλήρωση των υποχρεώσεων του υπεργολάβου επεξεργασίας σύμφωνα με τη σύμβασή του με τον εκτελούντα την επεξεργασία. Ο εκτελών την επεξεργασία γνωστοποιεί στον υπεύθυνο επεξεργασίας κάθε περίπτωση μη εκπλήρωσης των συμβατικών υποχρεώσεων του υπεργολάβου επεξεργασίας.
ε) Ο εκτελών την επεξεργασία συμφωνεί με τον υπεργολάβο επεξεργασίας ρήτρα δικαιούχου τρίτου, βάσει της οποίας —σε περίπτωση που ο εκτελών την επεξεργασία έπαυσε να υφίσταται από πραγματική ή νομική άποψη ή κατέστη αφερέγγυος— ο υπεύθυνος επεξεργασίας έχει το δικαίωμα να καταγγείλει τη σύμβαση με τον υπεργολάβο επεξεργασίας και να του δώσει εντολή να διαγράψει ή να επιστρέψει τα δεδομένα προσωπικού χαρακτήρα.

6.8. Διεθνείς διαβιβάσεις

α) Κάθε διαβίβαση δεδομένων σε τρίτη χώρα ή διεθνή οργανισμό από τον εκτελούντα την επεξεργασία πραγματοποιείται μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας ή προκειμένου να εκπληρωθεί ειδική απαίτηση του δικαίου της Ένωσης ή του κράτους μέλους στο οποίο υπόκειται ο εκτελών την επεξεργασία και εκτελείται σύμφωνα με τους όρους του κεφαλαίου V του κανονισμού (ΕΕ) 2016/679.
β) Ο υπεύθυνος επεξεργασίας συμφωνεί ότι στις περιπτώσεις που ο εκτελών την επεξεργασία προσλαμβάνει υπεργολάβο επεξεργασίας σύμφωνα με τη ρήτρα 7.7 για την εκτέλεση συγκεκριμένων δραστηριοτήτων επεξεργασίας (για λογαριασμό του υπευθύνου επεξεργασίας) και οι εν λόγω δραστηριότητες επεξεργασίας περιλαμβάνουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα κατά την έννοια του κεφαλαίου V του κανονισμού (ΕΕ) 2016/679, ο εκτελών την επεξεργασία και ο υπεργολάβος επεξεργασίας μπορούν να διασφαλίζουν τη συμμόρφωση με το κεφάλαιο V του κανονισμού (ΕΕ) 2016/679 μέσω της χρήσης τυποποιημένων συμβατικών ρητρών που έχει εκδώσει η Επιτροπή σύμφωνα με το άρθρο 46 παράγραφος 2 του κανονισμού (ΕΕ)

2016/679, υπό τον όρο ότι πληρούνται οι προϋποθέσεις για τη χρήση των εν λόγω τυποποιημένων συμβατικών ρητρών.

Ρήτρα 7

Συνδρομή στον υπεύθυνο επεξεργασίας

α) Ο εκτελών την επεξεργασία ενημερώνει αμέσως τον υπεύθυνο επεξεργασίας για κάθε αίτημα που έχει λάβει από υποκείμενο των δεδομένων. Δεν απαντά ο ίδιος στο αίτημα, εκτός αν λάβει σχετική εξουσιοδότηση από τον υπεύθυνο επεξεργασίας.

β) Ο εκτελών την επεξεργασία βοηθά τον υπεύθυνο επεξεργασίας στην εκπλήρωση της υποχρέωσής του να απαντά στα αιτήματα των υποκειμένων των δεδομένων για άσκηση των δικαιωμάτων τους, λαμβανομένης υπόψη της φύσης της επεξεργασίας. Κατά την εκπλήρωση των υποχρεώσεών του σύμφωνα με τα στοιχεία α) και β), ο εκτελών την επεξεργασία συμμορφώνεται με τις εντολές του υπευθύνου επεξεργασίας.

γ) Επιπρόσθετα στην υποχρέωση του εκτελούντος την επεξεργασία να βοηθά τον υπεύθυνο επεξεργασίας σύμφωνα με τη ρήτρα 8 στοιχείο β), ο εκτελών την επεξεργασία βοηθά επίσης τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις παρακάτω υποχρεώσεις, λαμβανομένων υπόψη της φύσης της επεξεργασίας δεδομένων και των πληροφοριών που διαθέτει ο εκτελών την επεξεργασία:

1) την υποχρέωση να διενεργεί εκτίμηση του αντικτύπου των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία των δεδομένων προσωπικού χαρακτήρα (εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων), όταν ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων·

2) την υποχρέωση να ζητεί τη γνώμη της/των αρμόδιας/-ων εποπτικής/-ών αρχής/-ών πριν από την επεξεργασία, όταν μια εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας·

3) την υποχρέωση να διασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα είναι ακριβή και επικαιροποιημένα, ενημερώνοντας χωρίς καθυστέρηση τον υπεύθυνο επεξεργασίας σε περίπτωση που ο εκτελών την επεξεργασία αντιληφθεί ότι τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται είναι ανακριβή ή παρωχημένα·

4) τις υποχρεώσεις που προβλέπονται στο άρθρο 32 του κανονισμού (ΕΕ) 2016/679.

δ) Τα συμβαλλόμενα μέρη καθορίζουν στο προσάρτημα III τα κατάλληλα τεχνικά και οργανωτικά μέτρα με τα οποία ο εκτελών την επεξεργασία υποχρεούται να βοηθά τον υπεύθυνο επεξεργασίας για την εφαρμογή της παρούσας ρήτρας, καθώς και το πεδίο εφαρμογής και την έκταση της απαιτούμενης βοήθειας.

Ρήτρα 8

Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα

8.1.Παραβίαση δεδομένων που αφορά δεδομένα που επεξεργάζεται ο υπεύθυνος επεξεργασίας

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο εκτελών την επεξεργασία συνεργάζεται με τον υπεύθυνο επεξεργασίας και τον βοηθά να συμμορφωθεί προς τις υποχρεώσεις του που απορρέουν από τα άρθρα 33 και 34 του κανονισμού (ΕΕ) 2016/679 λαμβανομένων υπόψη της φύσης της επεξεργασίας και των πληροφοριών που διαθέτει ο εκτελών την επεξεργασία.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα που αφορά δεδομένα που επεξεργάζεται ο υπεύθυνος επεξεργασίας, ο εκτελών την επεξεργασία βοηθά τον υπεύθυνο επεξεργασίας:
α) να γνωστοποιήσει την παραβίαση δεδομένων προσωπικού χαρακτήρα στην/στις αρμόδια/-ες εποπτική/-ές αρχή/-ές, αμελλητί από τη στιγμή που ο υπεύθυνος επεξεργασίας απέκτησε γνώση του γεγονότος, κατά περίπτωση/(εκτός αν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων)·
β) να συγκεντρώσει τις παρακάτω πληροφορίες, οι οποίες, σύμφωνα με το άρθρο 33 παράγραφος 3 του κανονισμού (ΕΕ) 2016/679, αναφέρονται στη γνωστοποίηση του υπευθύνου επεξεργασίας και πρέπει να περιλαμβάνουν κατ' ελάχιστο:

1) τη φύση των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα·

2) τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα·

3) τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Όταν και στον βαθμό που δεν είναι δυνατόν να παρασχεθούν όλες αυτές οι πληροφορίες ταυτόχρονα, στην αρχική γνωστοποίηση περιλαμβάνονται οι πληροφορίες που είναι διαθέσιμες τη δεδομένη στιγμή, ενώ πρόσθετες πληροφορίες παρέχονται σε μεταγενέστερο χρόνο και χωρίς αδικαιολόγητη καθυστέρηση μόλις καταστούν διαθέσιμες.
γ) να συμμορφωθεί, σύμφωνα με το άρθρο 34 του κανονισμού (ΕΕ) 2016/679, με την υποχρέωση να ανακοινώνει αμελλητί στο υποκείμενο των δεδομένων την παραβίαση δεδομένων προσωπικού χαρακτήρα, όταν αυτή ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

8.2. Παραβίαση δεδομένων που αφορά δεδομένα που επεξεργάζεται ο εκτελών την επεξεργασία

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα που αφορά δεδομένα που επεξεργάζεται ο εκτελών την επεξεργασία, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση από τη στιγμή που αποκτά γνώση της παραβίασης. Η εν λόγω γνωστοποίηση περιλαμβάνει κατ' ελάχιστο:

1. περιγραφή της φύσης της παραβίασης (συμπεριλαμβανομένων, όπου είναι δυνατόν, των κατηγοριών και του κατά προσέγγιση αριθμού των

επηρεαζόμενων υποκειμένων των δεδομένων και αρχείων δεδομένων)·

2. τα στοιχεία του σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες σχετικά με την παραβίαση των δεδομένων προσωπικού χαρακτήρα·

3. τις ενδεχόμενες συνέπειες και τα ληφθέντα ή προτεινόμενα προς λήψη μέτρα για την αντιμετώπιση της παραβίασης, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Όταν και στον βαθμό που δεν είναι δυνατόν να παρασχεθούν όλες αυτές οι πληροφορίες ταυτόχρονα, στην αρχική γνωστοποίηση περιλαμβάνονται οι πληροφορίες που είναι διαθέσιμες τη δεδομένη στιγμή, ενώ πρόσθετες πληροφορίες παρέχονται σε μεταγενέστερο χρόνο και χωρίς αδικαιολόγητη καθυστέρηση μόλις καταστούν διαθέσιμες.

Τα συμβαλλόμενα μέρη καθορίζουν στο προσάρτημα III όλα τα άλλα στοιχεία που πρέπει να παρέχονται από τον εκτελούντα την επεξεργασία κατά την παροχή βοήθειας στον υπεύθυνο επεξεργασίας για τη συμμόρφωση προς τις υποχρεώσεις του υπευθύνου επεξεργασίας σύμφωνα με τα άρθρα 33 και 34 του κανονισμού (ΕΕ) 2016/679.

ΤΜΗΜΑ III

ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Ρήτρα 9

Μη συμμόρφωση με τις ρήτρες και καταγγελία

1. Με την επιφύλαξη των διατάξεων του κανονισμού (ΕΕ) 2016/679, σε περίπτωση που ο εκτελών την επεξεργασία παραβιάζει τις υποχρεώσεις του σύμφωνα με τις παρούσες ρήτρες, ο υπεύθυνος επεξεργασίας μπορεί να δώσει εντολή στον εκτελούντα την επεξεργασία να αναστείλει την επεξεργασία δεδομένων προσωπικού χαρακτήρα έως ότου ο τελευταίος συμμορφωθεί με τις παρούσες ρήτρες ή καταγγελθεί η σύμβαση. Ο εκτελών την επεξεργασία ενημερώνει αμέσως τον υπεύθυνο επεξεργασίας σε περίπτωση που αδυνατεί να συμμορφωθεί με τις παρούσες ρήτρες, για οποιονδήποτε λόγο.

2. Ο υπεύθυνος επεξεργασίας έχει δικαίωμα να καταγγείλει τη σύμβαση στον βαθμό που αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τις παρούσες ρήτρες, αν:

   1) η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τον εκτελούντα την επεξεργασία ανεστάλη από τον υπεύθυνο επεξεργασίας σύμφωνα με το στοιχείο α) και η συμμόρφωση με τις παρούσες ρήτρες δεν αποκαταστάθηκε εντός εύλογου χρονικού διαστήματος και, σε κάθε περίπτωση, εντός ενός μηνός από την ημερομηνία της αναστολής·

   2) ο εκτελών την επεξεργασία παραβιάζει ουσιωδώς ή με τρόπο διαρκή τις παρούσες ρήτρες ή τις υποχρεώσεις του βάσει του κανονισμού (ΕΕ) 2016/679 ·

   3) ο εκτελών την επεξεργασία δεν συμμορφώνεται με δεσμευτική απόφαση αρμόδιου δικαστηρίου ή της/των αρμόδιας/-ων εποπτικής/-ών αρχής/-ών όσον αφορά τις υποχρεώσεις του σύμφωνα με τις παρούσες ρήτρες ή τον κανονισμό (ΕΕ) 2016/679.

3. Ο εκτελών την επεξεργασία έχει δικαίωμα να καταγγείλει τη σύμβαση στον βαθμό που αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τις παρούσες ρήτρες αν, παρόλο που έχει ενημερώσει τον υπεύθυνο επεξεργασίας ότι οι εντολές του παραβιάζουν εφαρμοστέες νομικές απαιτήσεις σύμφωνα με τη ρήτρα 7.1 στοιχείο β), ο υπεύθυνος επεξεργασίας εμμένει στη συμμόρφωση με τις εν λόγω εντολές.

4. Μετά την καταγγελία της σύμβασης, ο εκτελών την επεξεργασία, κατ' επιλογή του υπευθύνου επεξεργασίας, διαγράφει όλα τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται για λογαριασμό του υπευθύνου επεξεργασίας και πιστοποιεί στον υπεύθυνο επεξεργασίας ότι το έχει πράξει ή επιστρέφει όλα τα δεδομένα προσωπικού χαρακτήρα στον υπεύθυνο επεξεργασίας και διαγράφει τα υφιστάμενα αντίγραφα, εκτός αν το δίκαιο της Ένωσης ή του κράτους μέλους απαιτεί την αποθήκευση των δεδομένων προσωπικού χαρακτήρα. Έως τη διαγραφή ή την επιστροφή των δεδομένων, ο εκτελών την επεξεργασία συνεχίζει να διασφαλίζει τη συμμόρφωση με τις παρούσες ρήτρες.

ΠΡΟΣΑΡΤΗΜΑ Ι

Κατάλογος συμβαλλόμενων μερών

Υπεύθυνος επεξεργασίας: Το ΝΠΔΔ με την επωνυμία «Τεχνικό Επιμελητήριο Ελλάδας», που εδρεύει στον Δήμο Αθηναίων επί της οδού Νίκης, αρ. 4, Τ.Κ. 105 63, με Α.Φ.Μ. 090002260, υπαγόμενο στη ΔΟΥ Δ΄ Αθηνών

Υπογραφή και ημερομηνία προσχώρησης: η ημερομηνία υπογραφής της Κύριας Σύμβασης στην οποία προσαρτάται το παράρτημα

Υπεύθυνος Προστασίας Δεδομένων
1. Όνομα: Νικόλας Κανελλόπουλος – Χαρά Ζέρβα & Συνεργάτες Δικηγορική Εταιρεία
Διεύθυνση: Ομήρου 34, Αθήνα, Τ.Κ. 106 72
Όνομα, θέση και στοιχεία επικοινωνίας του υπευθύνου επικοινωνίας: Στέργιος Κωνσταντίνου, Άλκηστη Κωστοπούλου, dpo@central-tee.gr

Εκτελών την επεξεργασία: Η εταιρεία με την επωνυμία **«NEUROPUBLIC Ανώνυμη Εταιρεία Πληροφορικής και Επικοινωνιών»** και το διακριτικό τίτλο **«NEUROPUBLIC ΑΕ»** που εδρεύει στον Πειραιά, επί της οδού Μεθώνης 6,Τ.Κ 18545, με ΑΦΜ 999608870, υπαγόμενη στη ΔΟΥ ΦΑΕ ΠΕΙΡΑΙΑ

Υπογραφή και ημερομηνία προσχώρησης: η ημερομηνία υπογραφής της Κύριας Σύμβασης στην οποία προσαρτάται το παράρτημα

Υπεύθυνος Προστασίας Δεδομένων
1. Όνομα: Μαρία Καραφέρη του Κωνσταντίνου, δικηγόρος.
Διεύθυνση: Κολοκοτρώνη 62-64, Πειραιάς, Τ.Κ. 18531.
Όνομα, θέση και στοιχεία επικοινωνίας του υπευθύνου επικοινωνίας: Μαρία Καραφέρη, dpo@neuropublic.gr

ΤΑ ΣΥΜΒΑΛΛΟΜΕΝΑ ΜΕΡΗ

Για το ΤΕΕ	Για την Ανάδοχο
Ο Πρόεδρος	Η Νόμιμη Εκπρόσωπος
Γιώργος Ν. Στασινός	Ρόζα Γαργαλάκου

ΠΡΟΣΑΡΤΗΜΑ ΙΙ

Περιγραφή της επεξεργασίας

Κατηγορίες υποκειμένων δεδομένων των οποίων τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία:

- Υπάλληλοι ΤΕΕ
- Μέλη της Διοικούσας Επιτροπής του ΤΕΕ
- Αντισυμβαλλόμενοι του ΤΕΕ
- Μέλη του ΤΕΕ
- Οποιαδήποτε κατηγορία κρίνεται απαραίτητη για την εκτέλεση της Σύμβασης , όπως αυτή ορίζεται στο άρθρο 1

Κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία:

- Στοιχεία ταυτοποίησης (ονοματεπώνυμο, πατρώνυμο, μητρώνυμο, ΑΔΤ, ΑΦΜ)
- Στοιχεία τιμολόγησης (διεύθυνση, ΔΟΥ, ΚΑΔ)
- Στοιχεία επικοινωνίας (τηλέφωνο, email)
- Αριθμός Μητρώου ΤΕΕ
- Ιδιότητα/θέση
- Υπογραφή
- Τραπεζικός λογαριασμός
- Ποσά αμοιβών/αποδοχών
- Όνομα χρήστη
- Οποιαδήποτε κατηγορία δεδομένων εμπεριέχεται στα δικαιολογητικά των αντισυμβαλλομένων για την υποβολή προσφοράς, την κατάρτιση της σύμβασης και την πληρωμή των παραστατικών (π.χ. βιογραφικά, υπεύθυνες δηλώσεις, ποινικό μητρώο, φορολογική/ασφαλιστική ενημερότητα)
- Οποιαδήποτε κατηγορία δεδομένων εμπεριέχεται στις συμβάσεις του ΤΕΕ με τρίτους
- Οποιαδήποτε κατηγορία δεδομένων εμπεριέχεται στα παραστατικά των αντισυμβαλλομένων
- Οποιαδήποτε κατηγορία δεδομένων εμπεριέχεται στα χρηματικά εντάλματα
- Οποιαδήποτε κατηγορία δεδομένων εμπεριέχεται στη μισθοδοσία και τις βεβαιώσεις αποδοχών των υπαλλήλων
- Οποιαδήποτε κατηγορία κρίνεται απαραίτητη για την εκτέλεση της Σύμβασης , όπως αυτή ορίζεται στο άρθρο 1

Ευαίσθητα δεδομένα που υποβάλλονται σε επεξεργασία και περιορισμοί ή εγγυήσεις που εφαρμόζονται ώστε να λαμβάνονται πλήρως υπόψη η φύση των δεδομένων και οι υφιστάμενοι κίνδυνοι, όπως, για παράδειγμα, αυστηρός περιορισμός του σκοπού, περιορισμοί στην πρόσβαση (συμπεριλαμβανομένης της πρόσβασης αποκλειστικά από προσωπικό που έχει λάβει εξειδικευμένη κατάρτιση), τήρηση αρχείου πρόσβασης στα δεδομένα, περιορισμοί στις περαιτέρω διαβιβάσεις ή πρόσθετα μέτρα ασφάλειας: Δεν υφίστανται πρόσθετα μέτρα ασφάλειας, διότι το σύνολο των δεδομένων τυγχάνει επεξεργασίας ως ειδικής κατηγορίας.

Δεδομένα υγείας (στο πλαίσιο χορήγησης επιδομάτων υγείας)

Φύση της επεξεργασίας

Πρόσβαση, Καταχώριση, Αποθήκευση, Μεταβολή, Ανάκτηση, Χρήση, Διαγραφή και κάθε επεξεργασία που κρίνεται απαραίτητη σύμφωνα με το αντικείμενο της Σύμβασης, όπως αυτό ορίζεται στο άρθρο 1.

Σκοπός/-οί για τον οποίο ή τους οποίους τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για λογαριασμό του υπευθύνου επεξεργασίας.

Η παροχή υπηρεσιών σχετικά με το πληροφοριακό σύστημα διαχείρισης δαπανών του ΤΕΕ, όπως ειδικότερα προβλέπεται στο άρ. 1 της Σύμβασης.

Διάρκεια της επεξεργασίας

Η προβλεπόμενη διάρκεια στο άρθρο 2 της Σύμβασης.

ΠΡΟΣΑΡΤΗΜΑ ΙΙΙ

Τεχνικά και οργανωτικά μέτρα, συμπεριλαμβανομένων των τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας των δεδομένων

Τεχνικά και οργανωτικά μέτρα ασφάλειας

Η παρούσα σύμβαση αφορά σε υπηρεσίες σχετικές με το σύστημα διαχείρισης δαπανών του ΤΕΕ, που υλοποιούνται με την εγκατάσταση πληροφοριακού συστήματος διαχείρισης δαπανών είτε στις εγκαταστάσεις του ΤΕΕ είτε στο κυβερνητικό νέφος. Το σύστημα θα ενσωματώνει τα μέτρα ασφάλειας που εφαρμόζει το ΤΕΕ στην πληροφοριακή και δικτυακή υποδομή του είτε τα αντίστοιχα του κυβερνητικού νέφους.

Κατά συνέπεια, το παρόν αναλύει τα μέτρα ασφάλειας που λαμβάνει ο Ανάδοχος και αφορούν στην ανάπτυξη και συντήρηση των εφαρμογών διαχείρισης δαπανών και τα μέτρα ασφάλειας που λαμβάνει ο Ανάδοχος για τις εγκαταστάσεις του και το προσωπικό του.

Μέτρα ασφάλειας σχετικά με την ανάπτυξη και συντήρηση των εφαρμογών διαχείρισης δαπανών

Στο πλαίσιο του έργου θα διατεθεί πλήρες σύστημα ασφάλειας, το οποίο θα ενορχηστρώνει τις λειτουργικές δυνατότητες του παρεχόμενου κεντρικού συστήματος διαχείρισης χρηστών και τις εγγενώς υποστηριζόμενες λειτουργίες διαχείρισης ασφάλειας του χρησιμοποιούμενου λογισμικού υποδομής, σε ένα ενιαίο υποσύστημα ασφάλειας, μέσω του οποίου θα επιτρέπεται η διαβαθμισμένη πρόσβαση στα επιμέρους υποσυστήματα και τις τηρούμενες και διακινούμενες πληροφορίες, ανάλογα με το ρόλο και την ομάδα κάθε χρήστη. Επιπλέον, και όπως περιγράφεται αναλυτικά ακολούθως, θα παρέχονται εξελιγμένες δυνατότητες τήρησης ενιαίας αναλυτικής καταγραφής (auditing & logging) όλων των ενεργειών των χρηστών αναφορικά με τη συμπεριφορά τους στη πρόσβαση των δικτυακών τόπων, των αρχείων και τη χρήση των σεναρίων ροής εργασιών. Επί της διαδικασίας καταγραφής θα είναι δυνατή η δημιουργία αναλυτικών αναφορών σχετικά με τις ενέργειες των χρηστών που καταγράφηκαν.

Κατά το σχεδιασμό του Έργου η εταιρία μας θα λάβει ειδική μέριμνα και θα δρομολογηθούν οι κατάλληλες δράσεις για:

- την Ασφάλεια των Πληροφοριακών Συστημάτων, Εφαρμογών, Μέσων και Υποδομών,
- την προστασία της ακεραιότητας, εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών,
- την Αξιοπιστία του συνόλου του συστήματος, οπότε και θα διατεθούν οι κατάλληλοι μηχανισμοί backup και restore, απαιτείται μηχανισμός καταγραφής των κινήσεων των χρηστών (auditing, logging),
- δυνατότητα ελέγχου (revision / audit): κάθε τροποποίηση ή επεξεργασία των δεδομένων θα μπορεί να ελεγχθεί, δηλαδή από ποιόν έγινε και πότε,
- ευθύνη (accountability): θα προκύπτει ποιος είναι υπεύθυνος για την εισαγωγή, πρόσβαση ή τροποποίηση κάθε δεδομένου,
- διαφάνεια (transparency): θα γίνεται τεκμηρίωση των διαδικασιών της επεξεργασίας ώστε να μπορούν να ελεγχθούν,
- υλοποίηση της αρχιτεκτονικής «πολλαπλών επιπέδων ασφαλείας» (defence-in-depth) σε όλους τους τομείς του συστήματος αξιοποιώντας τις δυνατότητες των λειτουργικών συστημάτων, και των συσκευών ασφάλειας,

- μέριμνα για fault tolerance διάρθρωση του συστήματος, σε αποτυχίες/αστοχίες υλικού ή σε σφάλματα χειρισμού,
- πιστοποίηση (authentication): για τον έλεγχο αυθεντικότητας της ταυτότητας των μερών που ανταλλάσσουν δεδομένα,
- εξουσιοδότηση (authorization): για τη διασφάλιση διαδικασίας της πρόσβασης του χρήστη, στα δεδομένα,
- την προστασία των προς επεξεργασία και αποθηκευμένων προσωπικών δεδομένων αναζητώντας και εντοπίζοντας με μεθοδικό τρόπο τα τεχνικά μέτρα και τις οργανωτικο-διοικητικές διαδικασίες.
- λίστα σημείων ελέγχου της ασφάλειας του Συστήματος που θα παρακολουθούνται σε όλη τη διάρκεια του Έργου
- αναλυτική καταγραφή της διαδικασίας λήψης και τήρησης αντιγράφων ασφαλείας,
- Για το σχεδιασμό και την υλοποίηση των τεχνικών μέτρων ασφαλείας του Έργου, η εταιρία μας θα λάβει ιδιαίτερα υπόψη της:
- το θεσμικό και νομικό πλαίσιο που ισχύει σε εθνικό και κοινοτικό επίπεδο (π.χ. προστασία των προσωπικών δεδομένων Ν. 4624/2019), τον Κανονισμό Ε.Ε. 679/2016 και τις σύγχρονες εξελίξεις στις ΤΠΕ,
- την υφιστάμενη Πολιτική Ασφαλείας του Φορέα,
- τις βέλτιστες πρακτικές στο χώρο της Ασφάλειας στις ΤΠΕ (best practices), καθώς και τις κατευθυντήριες γραμμές στο πλαίσιο του Κανονισμού Ε.Ε. 679/2016.
- τα επαρκέστερα προϊόντα λογισμικού και υλικού
- τυχόν διεθνή de facto ή de jure σχετικά πρότυπα (π.χ. ISO/IEC 27001)

Κατά τη διάρκεια υλοποίησης του έργου δύναται τα τεχνικά μέτρα ασφάλειας που θα υλοποιηθούν από την εταιρία μας να επανεξετάζονται και να αναθεωρούνται κατά περίπτωση στο πλαίσιο διασφάλισης της καλής λειτουργίας του συστήματος και ύστερα από την έγκριση της Αναθέτουσας Αρχής.

Για την υλοποίηση των παραπάνω η εταιρία μας θα λάβει ειδική μέριμνα ώστε να γίνει με την ελάχιστη δυνατή παρεμπόδιση της λειτουργίας του ΤΕΕ και να επιφέρει τις ελάχιστες δυνατές τροποποιήσεις στις εφαρμογές και τα υπόλοιπα υποσυστήματα του Επιμελητηρίου.

Διαχείριση Ασφάλειας Πληροφοριών

Η NEUROUBLIC είναι πιστοποιημένη με το **EN ISO 27001:2013** με το **EN ISO 9001:2015** για δραστηριότητες που αφορούν τα παρακάτω πεδία εφαρμογής:

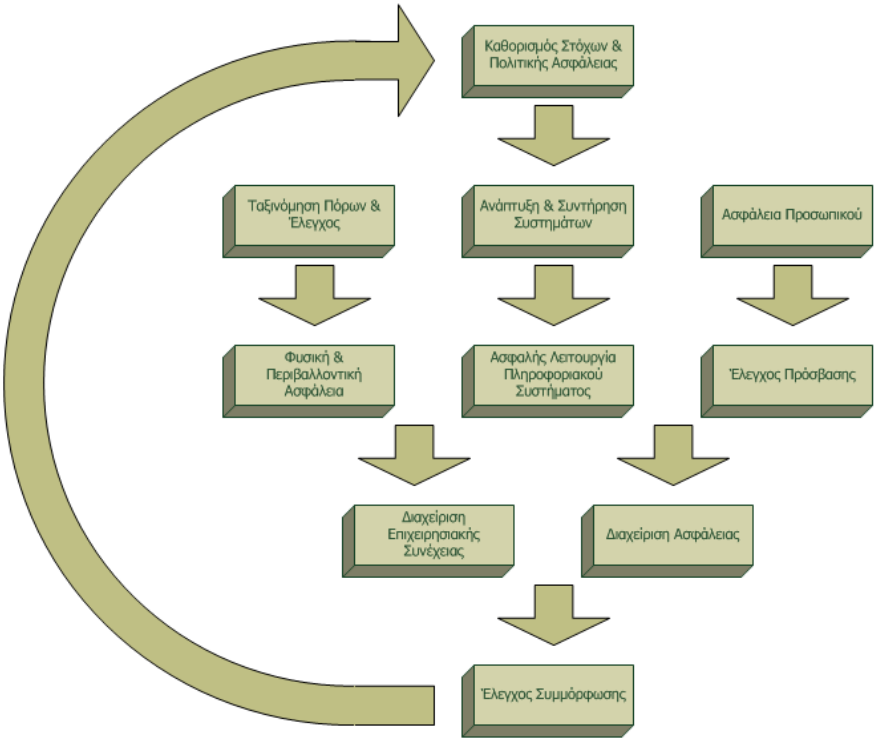
- Παροχή Υπηρεσιών στον αγροτικό τομέα
- **Παροχή Υπηρεσιών Φιλοξενίας Εφαρμογών**
- **Ανάλυση, Σχεδιασμός, Ανάπτυξη, Παραμετροποίηση, Εγκατάσταση, Συντήρηση, Τεχνική Υποστήριξη και Εκπαίδευση Χρηστών Συστημάτων Πληροφορικής**
- **Ανάλυση, Σχεδιασμός, Ανάπτυξη, παραμετροποίηση, Εγκατάσταση, Συντήρηση, Τεχνική Υποστήριξη και Εκπαίδευση Χρηστών Γεωγραφικών Συστημάτων Πληροφορικής**
- Σχεδιασμός, Κατασκευή, Εγκατάσταση, Συντήρηση και Υποστήριξη Σταθμών Τηλεμετρίας

Αναλυτικότερα, η εταιρία ανέπτυξε και εφαρμόζει σύστημα Διαχείρισης Ασφάλειας Πληροφοριών για τις δραστηριότητες της που έχουν σχέση με την Παροχή Φιλοξενίας Εφαρμογών και την Ανάπτυξη Πληροφοριακών Συστημάτων σύμφωνα με τις απαιτήσεις του προτύπου EN ISO 27001:2013 που διαθέτει. Η πιστοποίηση αυτή κατευθύνει και καθορίζει την Πολιτική στην οποία δεσμεύεται η Εταιρεία για την ασφάλεια των Πληροφοριών και ειδικότερα την ασφάλεια υπηρεσιών διαδικτύου.

Η NEUROPUBLIC A.E. είναι από τις ελάχιστες εταιρίες στην Ελλάδα και η πρώτη στον τομέα Ανάπτυξης και Φιλοξενίας Εφαρμογών που έχει πιστοποιηθεί και εφαρμόζει επί σειρά ετών το EN ISO 27001:2013.

Βάσει των απαιτήσεων του διεθνούς προτύπου ISO 27001:2013, για την εφαρμογή του οποίου είναι πιστοποιημένη η NeuroPublic A.E., παρουσιάζουμε το σύνολο των αλληλοσυμπληρούμενων διαδικασιών που καλύπτουν αυτές τις απαιτήσεις και έχουν προσαρμοστεί για τις απαιτήσεις του παρόντος έργου.

Οι διαδικασίες αυτές παρουσιάζονται διαγραμματικά στο ακόλουθο διάγραμμα:



Το διάγραμμα απεικονίζει μία κυκλική σειρά εκτέλεσης των διαδικασιών ασφάλειας για την ικανοποίηση των απαιτήσεων της διαχείρισης της ασφάλειας των πληροφοριών. Η πρακτική εφαρμογή ενός συστήματος διαχείρισης ασφάλειας των πληροφοριών απαιτεί την ανταπόκριση σε συμβάντα, η οποία μπορεί να απαιτεί την εκτός σειράς εκτέλεση μίας ή περισσοτέρων διαδικασιών.

Οι διαδικασίες περιγράφονται αναλυτικά στη συνέχεια.

<u>Καθορισμός Στόχων & Πολιτικής Ασφάλειας</u>

Σκοπός της διαδικασίας είναι ο καθορισμός συγκεκριμένων στόχων και πολιτικής ασφάλειας του έργου, εξασφαλίζοντας τη έμπρακτη ρύθμιση των ζητημάτων ασφάλειας σε όλα τα επίπεδα του.

Κείμενο της Πολιτικής Ασφάλειας

Το κείμενο της πολιτικής ασφάλειας θα πρέπει να γίνει αποδεκτό από την ΕΠΠΕ του έργου ή και από τα αρμόδια στελέχη της ΑΑ. Στη συνέχεια θα πρέπει να δημοσιοποιηθεί σε όλους τους εμπλεκόμενους στο έργο υπαλλήλους. Θα πρέπει να αναφέρει τη δέσμευση της ΑΑ και τον τρόπο προσέγγισης σε θέματα ασφάλειας και θα πρέπει τουλάχιστον να περιλαμβάνει τα ακόλουθα:

- τον ορισμό της ασφάλειας των πληροφοριών, το σκοπό της και τη σπουδαιότητά της ως μηχανισμού που επιτρέπει την ανταλλαγή πληροφοριών,
- τους σκοπούς της διοίκησης και την υποστήριξή της αναφορικά με την ασφάλεια,
- την επεξήγηση της πολιτικής ασφάλειας, των αρχών, των προτύπων και των απαιτήσεων που πρέπει να ικανοποιήσει ο φορέας, όπως σχετική νομοθεσία, προστασία από ιούς, επιπτώσεις μη συμμόρφωσης με την πολιτική ασφάλειας, διαχείριση επιχειρηματικής συνέχειας κλπ.,
- τον ορισμό γενικών και ειδικών καθηκόντων για τη διαχείριση της ασφάλειας και την αναφορά συμβάντων,
- αναφορές σε άλλα κείμενα που μπορούν να υποστηρίξουν την πολιτική ασφάλειας, όπως περιγραφές συγκεκριμένων διαδικασιών και κανονισμών.

Η πολιτική ασφάλειας θα πρέπει να κοινοποιείται σε ολόκληρη την ομάδα έργου, έχοντας κατά περίπτωση την κατάλληλη μορφή.

Ταξινόμηση Πόρων & Έλεγχος

Σκοπός είναι η κατάλληλη προστασία των πόρων του έργου. Όλοι οι κύριοι πόροι, σχετικοί με τα δεδομένα του έργου, θα έχουν έναν ορισμένο ιδιοκτήτη. Η υπευθυνότητα για τους πόρους του φορέα διασφαλίζει τη διατήρηση του κατάλληλου επιπέδου ασφάλειας.

Μέθοδος

Η καταγραφή των πόρων βοηθά στη σωστή προστασία τους και μπορεί να απαιτείται και για άλλους λόγους, όπως συμμόρφωση με τη νομοθεσία, ασφάλεια προσωπικού κλπ. Η διαδικασία της καταγραφής των πόρων του έργου αποτελεί σημαντικό τμήμα της διαδικασίας διαχείρισης κινδύνου. Για κάθε πόρο καθορίζεται ένας υπεύθυνος ιδιοκτήτης, καθώς επίσης και ένα επίπεδο ασφάλειας. Επιπλέον θα πρέπει να καταγράφεται και η τοποθεσία του. Κάθε πόρος ο οποίος αποκτάται από κάποιο τμήμα της του έργου, ο υπεύθυνος του υποχρεούται να το καταχωρήσει στον αντίστοιχο κατάλογο συμπληρώνοντας όλα τα αντίστοιχα υποχρεωτικά στοιχεία.

Σχετικά με τα πληροφοριακά συστήματα, έχουμε τους ακόλουθους σχετικούς πόρους:

- Πληροφοριακοί πόροι: βάσεις δεδομένων, αρχεία δεδομένων, εκπαιδευτικό υλικό, περιγραφή διαδικασιών, σχέδια επιχειρησιακής συνέχειας, εγχειρίδια κλπ.
- Λογισμικό: εφαρμογές, εργαλεία ανάπτυξης, λειτουργικά συστήματα κλπ.
- Φυσικοί πόροι: υλικό υπολογιστών, εξοπλισμός τηλεπικοινωνιών, αποθηκευτικά μέσα κλπ.
- Υπηρεσίες: ηλεκτρισμός, κλιματισμός, υπηρεσίες επεξεργασίας δεδομένων κλπ.

Πέραν του διαχωρισμού βάσει της υφής του πόρου, υπάρχει και η κλίμακα κινδύνου με την οποία οι πόροι κατηγοριοποιούνται βάσει της αξίας τους και του βαθμού στον οποίο είναι ευάλωτοι τόσο σε εξωτερικούς όσο και εσωτερικούς κινδύνους.

Επίπεδα προστασίας:

- Μέγιστο: αυτό είναι το επίπεδο όπου ομαδοποιούνται όλοι οι πόροι που έχουν άμεση σχέση με την ομαλή λειτουργία του Data Center, τα δεδομένα (προσωπικού ή μη χαρακτήρα) και το σχεδιασμό των εφαρμογών.
- Μεσαίο: εδώ κατηγοριοποιούνται όλοι οι πόροι οι οποίοι αντιστοιχούν σε σημαντικές αλλά όχι κρίσιμες λειτουργίες του έργου.
- Μικρό: στο χαμηλότερο επίπεδο ανήκουν όλοι οι υπόλοιποι πόροι.

Ανάπτυξη & Συντήρηση Συστημάτων

Σκοπός αυτής της διαδικασίας είναι η διασφάλιση ότι η ασφάλεια είναι υλοποιημένη μέσα στα πληροφοριακά συστήματα, η αποτροπή κατάχρησης, απώλειας ή αλλαγής των δεδομένων στις εφαρμογές του συστήματος, η προστασία της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των δεδομένων, η διασφάλιση ότι τα έργα πληροφορικής και οι εργασίες υποστήριξης γίνονται με ασφαλή τρόπο και η διατήρηση της ασφάλειας των εφαρμογών και των πληροφοριών.

Ανάλυση απαιτήσεων ασφάλειας και προδιαγραφές

Οι απαιτήσεις με βάση τις οποίες γίνεται η ανάπτυξη των εφαρμογών περιλαμβάνουν τις απαιτήσεις ασφάλειας και προστασίας προσωπικών δεδομένων, έτσι ώστε η ασφάλεια και η ιδιωτικότητα να ενσωματώνονται στις εφαρμογές «από το σχεδιασμό».

Ασφάλεια εφαρμογών

Σκοπός είναι η αποτροπή κατάχρησης, απώλειας ή αλλαγής των δεδομένων στις εφαρμογές του συστήματος. Οι μηχανισμοί καταγραφής των ενεργειών στο σύστημα είναι έτσι σχεδιασμένοι ώστε να καλύπτουν και τις εφαρμογές. Επίσης, περιλαμβάνουν τον έλεγχο της εγκυρότητας των προς εισαγωγή δεδομένων, την επεξεργασία τους και τα αποτελέσματα της τελευταίας.

Έλεγχος εγκυρότητας δεδομένων

Η εισαγωγή δεδομένων στις εφαρμογές ελέγχεται ώστε να είναι σωστή και να γίνεται με τον κατάλληλο τρόπο. Υλοποιούνται οι ακόλουθοι μηχανισμοί:

- Διπλή εισαγωγή δεδομένων ώστε να εντοπισθούν μη αποδεκτές τιμές ή χαρακτήρες, ανεπαρκή δεδομένα, χαρακτήρες ελέγχου (control) κλπ.
- Περιοδικός έλεγχος των περιεχομένων των πεδίων-κλειδιών για να επιβεβαιωθεί η ορθότητά τους.
- Έλεγχος των προς εισαγωγή δεδομένων για να εντοπιστεί κάποια μη εξουσιοδοτημένη αλλαγή.
- Διαδικασίες για την αναφορά λαθών.
- Έλεγχο της αληθοφάνειας των δεδομένων.
- Καθορισμό των ευθυνών του προσωπικού που εισάγει τα δεδομένα στο σύστημα.

- Έλεγχος της επεξεργασίας των δεδομένων
- Τα δεδομένα που έχουν εισαχθεί σωστά στο σύστημα μπορούν να παραποιηθούν από λάθη κατά την επεξεργασία τους ή από σκόπιμες ενέργειες. Στο σύστημα υπάρχουν ενσωματωμένες διαδικασίες για τον έλεγχο της εγκυρότητας των δεδομένων. Η σχεδίαση των εφαρμογών προβλέπει την προστασία των δεδομένων ώστε να ελαχιστοποιηθεί η πιθανότητα λάθους που μπορεί να οδηγήσει σε απώλεια της ακεραιότητας τους. Εξετάζονται και υλοποιούνται τα ακόλουθα:
    - Η θέση και η χρήση λειτουργιών των προγραμμάτων μέσω των οποίων μπορούν να γίνουν αλλαγές στα δεδομένα.
    - Διαδικασίες που να διασφαλίζουν τη σωστή σειρά εκτέλεσης των εφαρμογών και των απαραίτητων βημάτων για την αποκατάσταση κάποιας βλάβης.
    - Η χρήση των κατάλληλων προγραμμάτων για την αποκατάσταση των προβλημάτων που παρουσιάζονται στο σύστημα ώστε να διασφαλισθεί η σωστή επεξεργασία των δεδομένων.
    - Οι απαιτούμενοι μηχανισμοί ελέγχου εξαρτώνται από τη φύση των εφαρμογών και τις συνέπειες στον οργανισμό που απορρέουν από την απώλεια δεδομένων. Παραδείγματα ελέγχων είναι τα ακόλουθα:
        - Η δυνατότητα rollback για δοσοληψίες που γίνονται στο σύστημα.
        - Διαδικασίες ελέγχου της συνέχειας των δεδομένων (π.χ. έλεγχος κάποιου υπολοίπου σε σχέση με την τελευταία κίνηση).
        - Έλεγχος των δεδομένων που δημιουργούνται από το ίδιο το σύστημα.
        - Έλεγχος της ακεραιότητας των προγραμμάτων και των δεδομένων που μεταφέρονται ανάμεσα σε διαφορετικά συστήματα.
        - Συνόψεις (hashes) εγγραφών και αρχείων.
        - Έλεγχος ότι οι εφαρμογές τρέχουν τις κατάλληλες χρονικές περιόδους.
        - Έλεγχος ότι οι εφαρμογές εκτελούνται με τη σωστή σειρά και ότι σε περίπτωση λάθους η επεξεργασία σταματά μέχρι να λυθεί το πρόβλημα που παρουσιάστηκε.
        - Έλεγχος αποτελεσμάτων της επεξεργασίας

Τα αποτελέσματα της επεξεργασίας των δεδομένων στο σύστημα ελέγχονται προκειμένου να διασφαλιστεί η ορθότητα της επεξεργασίας. Συνήθως τα πληροφοριακά συστήματα λειτουργούν με το σκεπτικό ότι εφόσον οι εφαρμογές έχουν δοκιμασθεί επιτυχώς, τα αποτελέσματα της επεξεργασίας θα είναι πάντοτε σωστά. Σε κάποιες περιπτώσεις όμως αυτό δεν ισχύει. Εξετάζονται τα ακόλουθα:

- Η αληθοφάνεια των αποτελεσμάτων
- Η εναρμόνιση της επεξεργασίας όλων των δεδομένων.
- Η παροχή επαρκούς πληροφορίας προκειμένου να επιβεβαιώνεται η ακρίβεια και η ορθότητα των πληροφοριών.

- Διαδικασίες για την αντιμετώπιση λαθών.
- Ο καθορισμός των ευθυνών του προσωπικού που σχετίζεται με τις διαδικασίες των αποτελεσμάτων της επεξεργασίας των δεδομένων.

Έλεγχος των εφαρμογών που λειτουργούν σε παραγωγή

Η εγκατάσταση εφαρμογών σε συστήματα παραγωγής θα πρέπει να είναι ελεγχόμενη. Προκειμένου να περιοριστεί ο κίνδυνος κάποιου προβλήματος εξετάζονται τα ακόλουθα:

- Η αναβάθμιση των εφαρμογών παραγωγής γίνεται από το εξουσιοδοτημένο προσωπικό και κατόπιν άδειας της διοίκησης του έργου.
- Ο εκτελέσιμος κώδικας δοκιμάζεται διεξοδικά πριν εγκατασταθεί σε σύστημα παραγωγής. Επιπλέον θα πρέπει να προηγηθεί όποια άλλη αναβάθμιση είναι απαραίτητη για τη σωστή λειτουργία του.
- Τηρείται αρχείο με όλες τις αναβαθμίσεις που έχουν γίνει στις εφαρμογές παραγωγής.
- Παλαιότερες εκδόσεις των προγραμμάτων φυλάσσονται ως μέτρο επιχειρησιακής συνέχειας του φορέα.

Προστασία συστημάτων δοκιμών

Τα δεδομένα που προορίζονται για τις δοκιμές συστημάτων και εφαρμογών θα πρέπει να προστατεύονται επαρκώς, αφού συνήθως είναι παρεμφερή με τα δεδομένα παραγωγής. Δεν χρησιμοποιούνται δεδομένα που αναφέρονται σε πραγματικά πρόσωπα ή εάν χρησιμοποιηθούν τέτοια δεδομένα, πρώτα αφαιρούνται στοιχεία που να υποδεικνύουν συγκεκριμένα άτομα. Όταν πρόκειται να χρησιμοποιηθούν πραγματικά δεδομένα για τη διενέργεια δοκιμών χρησιμοποιούνται οι ακόλουθοι μηχανισμοί:

- Οι διαδικασίες ελέγχου πρόσβασης που ισχύουν για τα δεδομένα παραγωγής εφαρμόζονται και για τα δεδομένα δοκιμών.
- Υπάρχει ξεχωριστή εξουσιοδότηση κάθε φορά που πραγματικά δεδομένα αντιγράφονται σε συστήματα δοκιμών.
- Τα πραγματικά δεδομένα διαγράφονται από το σύστημα δοκιμών αμέσως μετά το πέρας της χρησιμότητάς τους.
- Έλεγχος της πρόσβασης στον κώδικα των εφαρμογών

Προκειμένου να ελαχιστοποιηθεί ο κίνδυνος μερικής ή ολικής καταστροφής των εφαρμογών, υπάρχει αυστηρός έλεγχος στην πρόσβαση του κώδικα των χρησιμοποιούμενων από την εταιρεία προγραμμάτων. Ελέγχονται τα ακόλουθα:

- Θα οριστεί ένας υπεύθυνος για τον πηγαίο κώδικα κάθε εφαρμογής.
- Το προσωπικό υποστήριξης δε έχει ελεύθερη πρόσβαση στον κώδικα των εφαρμογών.
- Ο κώδικας των εφαρμογών που είναι στη φάση της ανάπτυξης φυλάσσεται ξεχωριστά από τον κώδικα των εφαρμογών παραγωγής.
- Οποιαδήποτε αλλαγή στον πηγαίο κώδικα των εφαρμογών γίνεται σε συνεργασία με τον υπεύθυνο της εφαρμογής και κατόπιν ειδικής εξουσιοδότησης.

- Ο πηγαίος κώδικας είναι αποθηκευμένος σε ασφαλές περιβάλλον.
- Οι παλαιότερες εκδόσεις του κώδικα αρχειοθετούνται.
- Η συντήρηση και η αντιγραφή του πηγαίου κώδικα ελέγχεται αυστηρά.

Διαδικασίες ελέγχου αλλαγών

Η ομάδα έργου χρησιμοποιεί ένα σύνολο διαδικασιών για τη διενέργεια οποιασδήποτε αλλαγής στην εφαρμογή του συστήματος. Έτσι μειώνεται ο κίνδυνος δημιουργίας προβλημάτων στο σύστημα. Οι προγραμματιστές που αναπτύσσουν κάποια εφαρμογή έχουν πρόσβαση μόνο στα τμήματα του κώδικα που είναι απαραίτητα για τη δουλειά τους και οποιαδήποτε αλλαγή σε αυτά είναι κατάλληλα εξουσιοδοτημένη. Οι διαδικασίες με βάση τις οποίες γίνονται οι αλλαγές στην εφαρμογή περιλαμβάνουν τα ακόλουθα:

- Την τήρηση αρχείων με τα συμφωνημένα επίπεδα εξουσιοδότησης.
- Την εξασφάλιση ότι οι αλλαγές γίνονται από εξουσιοδοτημένους χρήστες.
- Την εξασφάλιση ότι οι αλλαγές δεν επηρεάζουν το υπάρχον επίπεδο ασφάλειας.
- Τον καθορισμό των εφαρμογών και των συστημάτων για τα οποία απαιτείται κάποια αλλαγή.
- Την παροχή εξουσιοδότησης πριν γίνει κάποια αλλαγή.
- Τη εξασφάλιση ότι οι λειτουργίες του φορέα θα επηρεαστούν όσο το δυνατόν λιγότερο.
- Την ενημέρωση των εγχειριδίων του συστήματος και των εφαρμογών και την αρχειοθέτηση ή την καταστροφή των παλαιών εγχειριδίων.
- Τη χρήση μηχανισμού ελέγχου των εκδόσεων (version control) για όλες τις αλλαγές.
- Την αλλαγή των διαδικασιών που χρησιμοποιούν οι χρήστες εφόσον κρίνεται απαραίτητο.

Η ομάδα έργου διαχωρίζει εντελώς το περιβάλλον δοκιμών από το περιβάλλον παραγωγής. Με αυτόν τον τρόπο έχει καλύτερο έλεγχο στις αλλαγές που γίνονται στο σύστημα και την προστασία των δεδομένων που χρησιμοποιούνται για δοκιμές.

Αναβαθμίσεις του λειτουργικού συστήματος

Περιοδικά είναι απαραίτητη η αναβάθμιση του λειτουργικού συστήματος που χρησιμοποιούν τα υπολογιστικά συστήματα του φορέα. Πριν όμως γίνει μια τέτοια αναβάθμιση θα πρέπει να ελεγχθεί κατά πόσο οι εφαρμογές του φορέα μπορούν να λειτουργήσουν με τη νέα έκδοση του λειτουργικού συστήματος. Αυτή η διαδικασία περιλαμβάνει τα ακόλουθα:

- Τον έλεγχο των εφαρμογών ώστε να διασφαλιστεί ότι δεν έχουν επηρεαστεί από τις αλλαγές του λειτουργικού συστήματος.
- Την εξασφάλιση οικονομικών πόρων για τις διαδικασίες που χρειάζονται για τη διενέργεια δοκιμών.
- Την έγκαιρη ενημέρωση για τις επικείμενες αλλαγές του λειτουργικού συστήματος ώστε να υπάρξει αρκετός χρόνος για τη δοκιμή των εφαρμογών στο καινούριο περιβάλλον.

- Τη διενέργεια των κατάλληλων αλλαγών του σχεδίου επιχειρησιακής συνέχειας του φορέα.
- Περιορισμοί στη διενέργεια αλλαγών

Εφόσον γίνουν κάποιες αλλαγές, η πρωτότυπη έκδοση της εφαρμογής θα πρέπει να διατηρείται. Οι αλλαγές θα πρέπει να γίνονται σε ένα αντίγραφο και να είναι πλήρως καταγεγραμμένες ώστε να εφαρμοσθούν ξανά αν είναι απαραίτητο σε κάποια αναβάθμιση της εφαρμογής

Ασφάλεια Προσωπικού

Σκοπός αυτής της διαδικασίας, είναι η ελαχιστοποίηση των κινδύνων που μπορεί να προκληθούν από ανθρώπινο λάθος, κλοπή, απάτη ή κατάχρηση των εγκαταστάσεων του έργου. Οι ευθύνες σχετικά με την ασφάλεια των πληροφοριών πρέπει να αναλύονται κατά τη διαδικασία πρόσληψης του προσωπικού. Επιπλέον πρέπει να αναφέρονται με σαφήνεια σε σχετικά συμβόλαια εργασίας, καθώς και να ελέγχεται η συμμόρφωση με αυτές κατά τη διάρκεια εργασίας του κάθε μέλους του προσωπικού. Οι υποψήφιοι υπάλληλοι πρέπει να ελέγχονται, ειδικά αυτοί που πρόκειται να έχουν ευαίσθητες θέσεις. Όλοι οι υπάλληλοι και οι συνεργάτες του έργου υπογράφουν συμφωνητικό για τήρηση εχεμύθειας (non-disclosure agreement).

Έλεγχος Προσωπικού

Κατά την υποβολή αιτήσεων από τους υποψήφιους εργαζόμενους, ο υπεύθυνος του έργου, πρέπει να ελέγχει και να επιβεβαιώνει τα όσα αναφέρονται σε αυτές. Πρέπει να ελέγχεται ότι:

- Υπάρχουν οι κατάλληλες συστάσεις.
- Τα στοιχεία που αναφέρονται στο βιογραφικό σημείωμα του υποψηφίου είναι ακριβή.
- Ο υποψήφιος κατέχει τους τίτλους που αναφέρει.
- Περιλαμβάνεται αποδεικτικό της ταυτότητας του υποψηφίου.

Συμφωνίες τήρησης της εχεμύθειας

Όλο το προσωπικό της NEUROPUBLIC υπογράφει συμφωνητικό εχεμύθειας είτε ως ξεχωριστό συμφωνητικό είτε στο πλαίσιο της σύμβασης εργασίας που υπογράφει.

Αντιμετώπιση περιστατικών

Σκοπός είναι η ελαχιστοποίηση των επιπτώσεων από περιστατικά ασφάλειας και η απόκτηση εμπειρίας από αυτά. Τα συμβάντα σχετικά με την ασφάλεια του έργου θα πρέπει να αναφέρονται άμεσα μέσα από κατάλληλους διαύλους επικοινωνίας του έργου. Όλοι οι υπάλληλοι πρέπει να γνωρίζουν τις διαδικασίες αναφοράς συμβάντων (παραβίαση ασφάλειας, απειλή, αδυναμία ή λάθος λειτουργία) που μπορούν να έχουν επιπτώσεις στην ασφάλεια των πόρων του έργου. Υπάρχουν τα σχετικά έγγραφα τα οποία μπορούν να χρησιμοποιούν ώστε να κατατίθενται στους υπευθύνους. Οι υπάλληλοι πρέπει να αναφέρουν άμεσα οτιδήποτε δουν ή τους κινήσει την υποψία στη διοίκηση του έργου. Για την κατάλληλη αντιμετώπιση τέτοιων συμβάντων, πρέπει να συλλέγονται και όλα τα αποδεικτικά στοιχεία.

Αναφορά συμβάντων

Τα συμβάντα που σχετίζονται με την ασφάλεια του οργανισμού και των φιλοξενούμενων δεδομένων πρέπει να αναφέρονται, το συντομότερο, μέσω των κατάλληλων διαύλων επικοινωνίας του έργου. Σε τέτοια περίπτωση, θα ακολουθήσουμε τη συγκεκριμένη διαδικασία «αναφοράς συμβάντων». Όλοι οι υπάλληλοι πρέπει να γνωρίζουν την συγκεκριμένη διαδικασία και πρέπει να την χρησιμοποιούν άμεσα σε περίπτωση προβλήματος με την ασφάλεια. Επιπλέον πρέπει να γίνεται και ενημέρωση των χρηστών για τα αποτελέσματα των αναφορών τους, τις αιτίες των αναφερθέντων προβλημάτων και πως μπορούν να αποφευχθούν στο μέλλον

Αναφορά αδυναμιών ασφάλειας

Οι χρήστες του συστήματος πρέπει να αναφέρουν κάθε αδυναμία ή πιθανή απειλή του συστήματος την οποία παρατηρούν ή υποπτεύονται. Η αναφορά πρέπει να γίνεται απευθείας στον υπεύθυνο του έργου και στον υπεύθυνο της ασφάλειας της πληροφορίας. Οι χρήστες σε καμία περίπτωση δε πρέπει να επιδεικνύουν κάποια πιθανή αδυναμία του συστήματος, γιατί κάτι τέτοιο μπορεί να ερμηνευθεί ως πιθανή υποβοήθηση εκδήλωσης επίθεση στο σύστημα.

Φυσική & Περιβαλλοντική Ασφάλεια

Σκοπός της παρούσας διαδικασίας είναι η αποτροπή μη εξουσιοδοτημένης πρόσβασης στις εγκαταστάσεις και το πληροφοριακό σύστημα του έργου, η πρόληψη απώλειας, ζημιών, έκθεσης των πόρων του έργου και της διακοπής των επιχειρησιακών δραστηριοτήτων του έργου και η αποτροπή υποκλοπής ή και κλοπής των πληροφοριών ή τμήματος των εγκαταστάσεων του έργου.

Ασφαλής Λειτουργία των Πληροφοριακών Συστημάτων

Σκοπός της παρούσας διαδικασίας είναι η σωστή και ασφαλής λειτουργία του ΟΠΣΟΥ, η ελαχιστοποίηση των βλαβών του συστήματος, η προστασία της ακεραιότητας του συστήματος, όπως και των πληροφοριών, η διατήρηση της ακεραιότητας και της διαθεσιμότητας του πληροφοριακού συστήματος, η ασφάλεια των πληροφοριών που υπάρχουν στο δίκτυο του φορέα, η αποτροπή ζημιών στους πόρους της και παρεμβολών στις λειτουργίες της και η προστασία των πληροφοριών που ανταλλάσσονται.

Διαδικασίες λειτουργίας και καθήκοντα

Τα καθήκοντα και οι διαδικασίες για τη διαχείριση και τη λειτουργία πληροφοριακού συστήματος είναι σαφώς καθορισμένα, συμπεριλαμβανομένων των ενεργειών που πρέπει να ακολουθούνται όταν προκύπτει ένα συμβάν ασφάλειας, το διαχωρισμό των καθηκόντων αλλά και τη συμμετοχή εξωτερικών συνεργατών. Επ’ αυτού περιλαμβάνονται ειδικές διαδικασίες στην περίπτωση κάποιου συμβάντος που να απειλεί την ασφάλεια του συστήματος.

Καταγραφή διαδικασιών λειτουργίας

Οι διαδικασίες που σχετίζονται με τη λειτουργία πληροφοριακού συστήματος και αναφέρονται στην πολιτική ασφάλειας του έργου, είναι αναλυτικά καταγεγραμμένες. Οι διαδικασίες αυτές περιγράφονται στις αναλυτικές οδηγίες εκτέλεσης όλων των εργασιών συμπεριλαμβανομένων των ακολούθων:

- διαχείριση και επεξεργασία πληροφοριών,
- χρονοδιαγράμματα εκτέλεσης εργασιών και ειδικά τη σχέση της κάθε εργασίας με άλλες, όπως και τους χρόνους ολοκλήρωσής της,

- οδηγίες για την αντιμετώπιση λαθών που μπορεί να προκύψουν κατά τη λειτουργία του συστήματος,
- συμβόλαια υποστήριξης για τον εξοπλισμό,
- οδηγίες χειρισμού ειδικού εξοπλισμού ή ευαίσθητων πληροφοριών,
- διαδικασίες επανεκκίνησης ή επαναφοράς του συστήματος στην περίπτωση κάποιου προβλήματος.
- διαδικασίες καθημερινής χρήσης του συστήματος, όπως εκκίνηση και τερματισμός λειτουργίας, τακτική συντήρηση, εφεδρική λήψη αντιγράφων κλπ.

Έλεγχος αλλαγών

Οι αλλαγές σε πληροφοριακό σύστημα ελέγχονται, καθώς αποτελούν αρκετά συχνά αιτία προβλημάτων. Υπάρχουν επίσημες διαδικασίες και καθήκοντα, μέσω των οποίων ελέγχονται όλες οι αλλαγές σε εξοπλισμό, λογισμικό και διαδικασίες στο σύστημα. Τηρούνται αναλυτικά αρχεία με τις αλλαγές του συστήματος. Κατά συνέπεια εξετάζονται οι ακόλουθοι μηχανισμοί:

- αναλυτική καταγραφή όλων των σημαντικών αλλαγών,
- έλεγχος των πιθανών συνεπειών τέτοιων αλλαγών,
- επίσημη διαδικασία έγκρισης των προτεινόμενων αλλαγών,
- κοινοποίηση όλων των σχετικών λεπτομερειών στα αρμόδια στελέχη του φορέα,
- διαδικασίες επαναφοράς του συστήματος στην περίπτωση ανεπιτυχών αλλαγών.

Διαχωρισμός καθηκόντων

Ο διαχωρισμός των καθηκόντων είναι μια μέθοδος για τη μείωση του κινδύνου κατάχρησης του συστήματος, είτε από αμέλεια είτε από δόλο. Ο διαχωρισμός των καθηκόντων διαχείρισης ή εκτέλεσης διάφορων επιχειρηματικών λειτουργιών είναι επίσης ένας μηχανισμός που εξετάζεται από την ομάδα διαχείρισης ασφάλειας προκειμένου να ελαχιστοποιηθούν οι πιθανότητες κατάχρησης ή μη εξουσιοδοτημένων αλλαγών στα δεδομένα ή τις υπηρεσίες. Λαμβάνεται ειδική μέριμνα ώστε κανένας να μην μπορεί να διενεργήσει απάτη, μόνος του, χωρίς να γίνει αντιληπτός. Η εξουσιοδότηση κάποιας ενέργειας και η εκτέλεσή της γίνονται από διαφορετικά άτομα και επ’ αυτού τηρούνται τα ακόλουθα:

- Υπάρχει διαχωρισμός των καθηκόντων όπου είναι απαραίτητη η συνεργασία για τον εντοπισμό απάτης, όπως στην περίπτωση παραγγελίας και παραλαβής αγαθών.
- Για την αποφυγή συγκάλυψης, υπάρχουν μηχανισμοί που να εμπλέκουν πολλά άτομα ώστε να μειωθεί ο κίνδυνος τέτοιων συνεργασιών.
- Διαχωρισμός των εγκαταστάσεων δοκιμών και λειτουργιών. Η ανάπτυξη και οι δοκιμές εφαρμογών μπορούν να προκαλέσουν μεγάλα προβλήματα σε πληροφοριακό σύστημα. Κρίνεται λοιπόν απαραίτητη η ύπαρξη διαχωρισμού ανάμεσα στα περιβάλλοντα ανάπτυξης, δοκιμών και παραγωγής. Για την προστασία του συστήματος παραγωγής, η ομάδα ασφάλειας του έργου θα εξετάσει και θα ελέγχει τα ακόλουθα:

- Οι εφαρμογές που είναι σε φάση ανάπτυξης η δοκιμών θα πρέπει να τρέχουν σε ξεχωριστά συστήματα από αυτό των παραγωγικών λειτουργιών.
- Η ανάπτυξη και οι δοκιμές των εφαρμογών θα πρέπει να είναι όσο το δυνατό πιο πολύ διαχωρισμένες.
- Τα εργαλεία ανάπτυξης λογισμικού δε θα πρέπει να είναι προσπελάσιμα από τα παραγωγικά συστήματα.
- Θα πρέπει να υπάρχουν διαφορετικές διαδικασίες login στα συστήματα παραγωγής, τα συστήματα δοκιμών και τα συστήματα ανάπτυξης.
- Το προσωπικό πληροφορικής θα πρέπει να έχει πρόσβαση μόνο στα απολύτως απαραίτητα μέρη των συστημάτων παραγωγής, στα οποία και θα πρέπει να υπάρχουν ειδικοί μηχανισμοί για λειτουργίες υποστήριξης.

Σχεδιασμός και αποδοχή συστήματος

Σκοπός είναι η ελαχιστοποίηση των βλαβών κάποιου πληροφοριακού συστήματος. Ο προσεκτικός σχεδιασμός και η κατάλληλη προετοιμασία, είναι απαραίτητα στοιχεία για τη διαθεσιμότητα πόρων και χωρητικότητας σε κάθε πληροφοριακό σύστημα του έργου. Θα πρέπει να γίνουν προβλέψεις των μελλοντικών απαιτήσεων από το σύστημα, ώστε να μειωθεί ο κίνδυνος υπερφόρτωσής του. Τα νέα συστήματα θα πρέπει να δοκιμάζονται με βάση τις καταγεγραμμένες λειτουργικές ανάγκες του έργου, πριν γίνουν αποδεκτά και τεθούν σε παραγωγική λειτουργία.

Αποδοχή συστήματος

Τα κριτήρια αποδοχής για τα νέα πληροφοριακά συστήματα, τις αναβαθμίσεις ή τις νέες εκδόσεις τους, είναι προκαθορισμένα με σαφήνεια, καταγεγραμμένα, δοκιμασμένα και συμφωνημένα και με βάση αυτά γίνονται οι σχετικές δοκιμές. Κατά συνέπεια εξετάζονται τα ακόλουθα:

- απαιτήσεις χωρητικότητας και απόδοσης
- διαδικασίες αντιμετώπισης προβλημάτων
- προετοιμασία και δοκιμή διαδικασιών ρουτίνας σε σχέση με τα καθορισμένα πρότυπα
- ύπαρξη των συμφωνημένων μηχανισμών ασφάλειας
- χειροκίνητες διαδικασίες
- διαδικασίες επιχειρηματικής συνέχειας
- εκπαίδευση στη χρήση του νέου συστήματος.

Εφεδρικό αντίγραφο ασφαλείας του συστήματος

Γίνεται τακτική λήψη εφεδρικών αντιγράφων των συστημάτων, ειδικότερα των κρίσιμων αρχείων και προγραμμάτων. Υπάρχουν οι επαρκείς πόροι για τη λήψη εφεδρικών αντιγράφων των συστημάτων, όπως επίσης γίνονται τακτικές δοκιμές ώστε να διασφαλίζεται η ικανοποίηση των αναγκών του έργου. Εξετάζονται και ελέγχονται οι ακόλουθοι μηχανισμοί:

- Ένα μέρος του εφεδρικού αντιγράφου και τα εγχειρίδια των διαδικασιών ανάκτησης φυλάσσονται σε ένα απομακρυσμένο σημείο, στο Data Center, ώστε

να αντιμετωπιστεί το ενδεχόμενο καταστροφής στη κύρια εγκατάσταση του φορέα. Τηρούνται τουλάχιστον τρία διαφορετικά εφεδρικά αντίγραφα των κρίσιμων στοιχείων και εφαρμογών του φορέα.

- Τα αποθηκευτικά μέσα που περιέχουν εφεδρικά αντίγραφα, προστατεύονται σύμφωνα με τα πρότυπα ασφάλειας του φορέα, είτε φυλάσσονται σε απομακρυσμένο σημείο, είτε στους κύριους χώρους του φορέα.
- Γίνεται τακτικός έλεγχος των μέσων που χρησιμοποιούνται για εφεδρικά αντίγραφα.
- Οι διαδικασίες ανάκτησης δοκιμάζονται τακτικά για να ελεγχθεί η αποτελεσματικότητά τους σε σχέση με τις απαιτήσεις του έργου. Επίσης καθορίζεται η χρονική διάρκεια διατήρησης ενός εφεδρικού αντίγραφου.

Το προσωπικό που διαχειρίζεται τα πληροφοριακά συστήματα του φορέα τηρεί αρχεία με τις δραστηριότητες του. Τα αρχεία αυτά περιλαμβάνουν τα ακόλουθα:

- την ώρα έναρξης της λειτουργίας του συστήματος, όπως και του κλεισίματός του
- τα προβλήματα που παρουσιάστηκαν στο σύστημα και τις ενέργειες για την αντιμετώπισή τους
- επιβεβαίωση της σωστής διαχείρισης των δεδομένων και των αποτελεσμάτων της επεξεργασίας τους
- το όνομα του προσώπου που έκανε την καταχώρηση στο αρχείο.
- Τα αρχεία λειτουργίας του συστήματος ελέγχονται σε τακτά χρονικά διαστήματα για τη συμμόρφωσή τους με τα πρότυπα που έχει θέσει η ομάδα ασφάλειας.

Διαχείριση αποθηκευτικών μέσων που μπορεί να διαγραφεί το περιεχόμενο τους

Υπάρχουν οι κατάλληλες διαδικασίες, οι οποίες είναι καταγεγραμμένες με σαφήνεια, για τη διαχείριση αποθηκευτικών μέσων που μπορεί να διαγραφεί το περιεχόμενο τους, όπως είναι οι ταινίες και οι δίσκοι. Ελέγχονται τα ακόλουθα:

- Τα αποθηκευτικά μέσα που δεν περιέχουν χρήσιμα πλέον δεδομένα διαγράφονται.
- Τηρείται αρχείο της μεταφοράς των αποθηκευτικών μέσων εκτός των χώρων του έργου. Επιπλέον, υπάρχει η κατάλληλη εξουσιοδότηση για οποιαδήποτε τέτοια μεταφορά.
- Όλα τα αποθηκευτικά μέσα φυλάσσονται κατάλληλα, με ασφάλεια και σύμφωνα με τις οδηγίες του κατασκευαστή.

Απόσυρση αποθηκευτικών μέσων

Τα διάφορα αποθηκευτικά μέσα, μετά την απόσυρση από τη λειτουργία τους είτε καταστρέφονται πλήρως, είτε διαγράφονται όλα τα δεδομένα τους πριν επαναχρησιμοποιηθούν. Υλοποιούνται οι ακόλουθες διαδικασίες:

- Τα αποθηκευτικά μέσα που περιέχουν ευαίσθητες πληροφορίες φυλάσσονται κατά τη χρήση τους και αποσύρονται ή ανακυκλώνονται με ασφάλεια, όπως με τη χρήση καταστροφέων εγγράφων ή με ασφαλή διαγραφή δεδομένων από μαγνητικά μέσα πριν την επαναχρησιμοποίησή τους.

- Ειδική μεταχείριση δίνεται για τα διάφορα έγγραφα, αντίγραφα εγγράφων και εκτυπώσεις, τα μαγνητικά αποθηκευτικά μέσα (ταινίες, δισκέτες, δίσκους κλπ), τα οπτικά αποθηκευτικά μέσα (CD ROMs κλπ.), τα φύλλα καρμπόν, τον κώδικα των εφαρμογών, τα δεδομένα που χρησιμοποιούνται από τις εφαρμογές και τα εγχειρίδια των συστημάτων.
- Η καταστροφή και η απόσυρση ευαίσθητων αποθηκευτικών μέσων καταγράφεται και τηρείται σχετικό αρχείο.
- Όταν συγκεντρώνονται πολλά αποθηκευτικά μέσα για καταστροφή, θα πρέπει δίδεται ιδιαίτερη προσοχή γιατί είναι πιθανό συσσωρεμένες μη ευαίσθητες πληροφορίες, να αποκαλύπτουν περισσότερα στοιχεία από μια μικρή ποσότητα ευαίσθητων πληροφοριών.

Χειρισμός πληροφοριών

Υπάρχουν συγκεκριμένες διαδικασίες για το χειρισμό και την αποθήκευση των πληροφοριών, προκειμένου να προστατεύονται από μη εξουσιοδοτημένη προσπέλαση ή ακόμα και κατάχρηση. Οι διαδικασίες αυτές βασίζονται στο σύστημα κατηγοριοποίησης των πληροφοριών του έργου και καλύπτουν έγγραφα, υπολογιστικά συστήματα, τηλεπικοινωνίες, ταχυδρομείο κλπ. Εξετάζονται και υλοποιούνται τα ακόλουθα:

- Χειρισμός και κατηγοριοποίηση όλων των αποθηκευτικών μέσων.
- Μηχανισμοί ελέγχου πρόσβασης στις πληροφορίες.
- Τήρηση αρχείου της προσπέλασης στις πληροφορίες.
- Έλεγχος της συνοχής ανάμεσα στην επεξεργασία των πληροφοριών και των αποτελεσμάτων αυτής.
- Προστασία των δεδομένων σε όλα τα στάδια της επεξεργασίας τους.
- Χρήση και αποθήκευση των διάφορων αποθηκευτικών μέσων σύμφωνα με τις προδιαγραφές του κατασκευαστή.
- Ελαχιστοποίηση της διανομής των δεδομένων.
- Επισήμανση όλων των αντιγράφων των δεδομένων για την αποτελεσματική προστασία τους.
- Περιοδικός έλεγχος του καταλόγου των εξουσιοδοτημένων χρηστών των δεδομένων.
- Ασφάλεια των εγχειριδίων των συστημάτων

Έλεγχος Πρόσβασης

Σκοπός είναι ο έλεγχος της πρόσβασης στις πληροφορίες του έργου, καθώς και η προστασία κάθε πληροφοριακού του συστήματος από μη εξουσιοδοτημένη προσπέλαση. Οι πληροφορίες καθώς και η πρόσβαση σε αυτές θα πρέπει να ελέγχονται με βάση τις επιχειρησιακές ανάγκες και της απαιτήσεις ασφάλειας του έργου.

Μέθοδος

Η συγκεκριμένη διαδικασία περιλαμβάνει τον έλεγχο της πρόσβασης στις πληροφορίες του φορέα μέσα από την πολιτική ασφάλειας. Συγκεκριμένα, η εν λόγω διαδικασία εξετάζει και ελέγχει την πρόσβαση:

- των χρηστών ή τρίτων στο δίκτυο
- στο λειτουργικό σύστημα
- στις εφαρμογές
- στη χρήση του συστήματος και στα δεδομένα
- Διαχείριση της Πρόσβασης των Χρηστών

Δήλωση χρηστών

Η ομάδα ασφάλειας εφαρμόζει συγκεκριμένη διαδικασία για την αρχική δήλωση των χρηστών στο σύστημα. Η διαδικασία αυτή περιλαμβάνει τα ακόλουθα:

- Χρήση μοναδικών ID χρηστών, τα οποία και θα καθιστούν υπεύθυνους τους χρήστες για τις πράξεις τους στο σύστημα.
- Έλεγχο της εξουσιοδότησης του χρήστη από τον ιδιοκτήτη του συστήματος για τη χρήση των παρεχόμενων υπηρεσιών. Σε κάποιες περιπτώσεις (ευαίσθητων δεδομένων) χρησιμοποιείται επιπλέον και ειδική εξουσιοδότηση της διοίκησης του έργου.
- Έλεγχο ότι τα δικαιώματα που αποκτά ο χρήστης είναι σύμφωνα με τις απαιτήσεις της εργασίας του και επιπλέον δεν παρακάμπτουν την αρχή διαχωρισμού των καθηκόντων.
- Εξασφάλιση ότι οι υπηρεσίες δεν παρέχονται πριν ολοκληρωθούν οι διαδικασίες εξουσιοδότησης των χρηστών.
- Τήρηση αρχείου όλων των χρηστών του συστήματος.
- Άμεση διαγραφή των χρηστών που αποχωρούν από το έργο.
- Περιοδικό έλεγχο για την ύπαρξη ανενεργών ή διπλών λογαριασμών χρηστών στο σύστημα.
- Εξασφάλιση ότι δεν μπορεί να αποδοθεί σε πολλούς χρήστες το ίδιο ID.

Διαχείριση προνομιακών δικαιωμάτων

Ο καθορισμός και η χρήση των προνομιακών δικαιωμάτων προσπέλασης (οποιοδήποτε σύνολο δικαιωμάτων ή χαρακτηριστικών σε ένα πολυχρηστικό σύστημα, τα οποία επιτρέπουν την παράκαμψη των μηχανισμών ελέγχου του συστήματος), είναι ελεγχόμενος και περιορισμένος. Τα πολυχρηστικά συστήματα, τα οποία χρειάζονται προστασία απέναντι σε μη εξουσιοδοτημένη πρόσβαση, έχουν μια διαδικασία εξουσιοδότησης η οποία ελέγχει τα προνομιακά δικαιώματα. Η συγκεκριμένη διαδικασία εξετάζει τα ακόλουθα:

- τα προνομιακά δικαιώματα που συνδέονται με κάθε μέρος του συστήματος (εφαρμογές, λειτουργικό σύστημα κλπ.), όπως και οι χρήστες που πρέπει να τα χρησιμοποιούν, θα καθορίζονται επακριβώς.
- τα προνομιακά δικαιώματα παρέχονται μόνο σε όσους χρήστες και για όσο χρονικό διάστημα είναι απολύτως απαραίτητο.
- τη διαδικασία καταγραφής των προνομιακών χρηστών του συστήματος, οι λογαριασμοί των οποίων θα ενεργοποιούνται στο σύστημα αφού ολοκληρωθεί η διαδικασία εξουσιοδότησης.
- Οι εφαρμογές του συστήματος θα πρέπει να λειτουργούν με τέτοιο τρόπο ώστε να μην απαιτούν προνομιακά δικαιώματα από τους χρήστες.

- Τα προνομιακά δικαιώματα θα πρέπει να δίνονται σε λογαριασμούς διαφορετικούς από αυτούς που χρησιμοποιούν οι χρήστες για τις συνηθισμένες εργασίες τους στο σύστημα.
- Διαχείριση συνθηματικών (password)
    - Τα συνθηματικά είναι ο πλέον συνηθισμένος τρόπος για την επιβεβαίωση της ταυτότητας ενός χρήστη του συστήματος. Η διαχείριση των συνθηματικών βασίζεται σε συγκεκριμένες διαδικασίες, οι οποίες:
    - Εξασφαλίζουν ότι για νέους χρήστες του συστήματος, όπως και στις περιπτώσεις που κάποιος χρήστης ξεχάσει το συνθηματικό του, θα του παρέχεται ένα προσωρινό συνθηματικό, το οποίο αμέσως μετά τη χρήση του θα πρέπει να αλλαχθεί.
    - Εξασφαλίζουν ότι τα προσωρινά συνθηματικά θα παρέχονται στους χρήστες με ασφαλή τρόπο, ενώ οι τελευταίοι θα επιβεβαιώνουν την παραλαβή. Τα συνθηματικά δεν πρέπει ποτέ να αποθηκεύονται σε κάποιο υπολογιστικό σύστημα ή σε εκτεθειμένα σημεία.

Έλεγχος δικαιωμάτων χρηστών

Για τον περιοδικό έλεγχο των δικαιωμάτων των χρηστών στο σύστημα και προκειμένου να υπάρξει αποτελεσματικός έλεγχος στα δεδομένα και τις υπηρεσίες του συστήματος, η διοίκηση του έργου θα καταρτίσει συγκεκριμένη διαδικασία. Κατ' αυτόν τον τρόπο:

- Τα δικαιώματα των χρηστών ελέγχονται με την παρέλευση (6) μηνών και μετά από κάθε αλλαγή.
- Οι εξουσιοδοτήσεις για προνομιακά δικαιώματα ελέγχονται εντός τριμήνου.
- Τα προνομιακά δικαιώματα ελέγχονται επίσης ανά τακτά χρονικά διαστήματα ώστε να μην είναι δυνατή η μη εξουσιοδοτημένη απόκτηση δικαιωμάτων.
- Ευθύνες Χρηστών

Έλεγχος πρόσβασης στο λειτουργικό σύστημα

Σκοπός είναι η αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε κάθε σύστημα του έργου. Οι μηχανισμοί ασφάλειας που μπορεί διαθέτει κάθε σύστημα σε επίπεδο λειτουργικού συστήματος, χρησιμοποιούνται για τον περιορισμό της πρόσβασης στους διάφορους πόρους. Οι συγκεκριμένοι μηχανισμοί είναι σε θέση να:

- Αναγνωρίζουν και να επιβεβαιώνουν την ταυτότητα του χρήστη και αν είναι δυνατό και του τερματικού που αυτός χρησιμοποιεί.
- Καταγράφουν επιτυχείς και ανεπιτυχείς προσπάθειες πρόσβασης.
- Παρέχουν κατάλληλους μηχανισμούς για αυθεντικοποίηση, οι οποίοι θα πρέπει να είναι σύμφωνοι με την πολιτική του φορέα.
- Περιορίζουν το χρόνο πρόσβασης των χρηστών αν αυτό κρίνεται απαραίτητο.
- Αναγνώριση τερματικών

Διαδικασίες σύνδεσης στο σύστημα

Η πρόσβαση στις υπηρεσίες κάθε πληροφοριακού συστήματος αποκτάται μέσω ασφαλούς διαδικασίας εισόδου στο σύστημα (log-on). Η διαδικασία αυτή θα πρέπει:

- Να μην εμφανίζει στην οθόνη διάφορα χαρακτηριστικά της ταυτότητας του χρήστη ή του συστήματος, έως ότου ολοκληρωθεί επιτυχώς.
- Να εμφανίζει προειδοποιητικά μηνύματα που να ενημερώνουν ότι η πρόσβαση επιτρέπεται μόνο στους εξουσιοδοτημένους χρήστες του συστήματος.
- Να μην εμφανίζει βοηθητικά μηνύματα που θα μπορούσαν να χρησιμοποιηθούν από μη εξουσιοδοτημένους χρήστες.
- Να επιβεβαιώνει τις απαιτούμενες πληροφορίες αφού εισαχθούν όλες στο σύστημα. Σε περίπτωση λάθους να μην ενημερώνει ποια πληροφορία απορρίφθηκε από το σύστημα.
- Να περιορίζει τον αριθμό των δυνατών προσπαθειών του χρήστη για να συνδεθεί.
- Να περιορίζει το χρόνο που έχει ο χρήστης στη διάθεσή του για να κάνει log-on.

Μετά την επιτυχή ολοκλήρωση της διαδικασίας να εμφανίζει την ώρα u954 και την ημερομηνία της τελευταίας επιτυχούς προσπάθειας του χρήστη και τις όποιες μη επιτυχείς προσπάθειες έγιναν στο μεταξύ.

Παράλληλα, καταγράφει τις ανεπιτυχείς προσπάθειες, και επιβάλει ένα χρονικό όριο πριν επιτρέψει ξανά στο χρήστη να προσπαθήσει και να αποσυνδέει όλες τις πιθανές συνδέσεις επικοινωνίας.

Αυθεντικοποίηση χρηστών

Όλοι οι χρήστες κάθε συστήματος (διαχειριστές, προϊστάμενοι, χρήστες κλπ.), έχουν ένα μοναδικό αναγνωριστικό (user ID), για καθαρά προσωπική τους χρήση στο σύστημα. Με αυτόν τον τρόπο είναι δυνατός ο εντοπισμός του υπεύθυνου ατόμου για όλες τις δραστηριότητες που γίνονται στο πληροφοριακό σύστημα του φορέα. Επιπλέον, τα user IDs δεν πρέπει να φανερώνουν τα δικαιώματα του χρήστη στο σύστημα. Σε εξαιρετικές περιπτώσεις, και εφόσον κάτι τέτοιο είναι απαραίτητο για τον φορέα, μια ομάδα χρηστών μπορεί να μοιράζεται το ίδιο user ID για την εκτέλεση συγκεκριμένων εργασιών στο σύστημα. Σε μια τέτοια περίπτωση θα πρέπει να υπάρχει ειδική έγκριση από τη διοίκηση του έργου, όπως επίσης και να χρησιμοποιηθεί κάποιος μηχανισμός που θα καθορίζει τις ευθύνες των μελών της ομάδας.

Υπάρχουν διάφορες διαδικασίες αυθεντικοποίησης που μπορούν να χρησιμοποιηθούν για την επιβεβαίωση της ταυτότητας ενός χρήστη. Τα συνθηματικά είναι ο πλέον συνηθισμένος τρόπος ο οποίος βασίζεται στη χρήση ενός μυστικού, γνωστού μόνο στο χρήστη. Άλλοι μηχανισμοί αυθεντικοποίησης περιλαμβάνουν συνδυασμούς κρυπτογραφίας και πρωτοκόλλων εξακρίβωσης της ταυτότητας του χρήστη. Διάφορα αντικείμενα, όπως έξυπνες κάρτες, τα οποία έχει στην κατοχή του ο χρήστης, μπορούν επίσης να χρησιμοποιηθούν για αυθεντικοποίηση στο σύστημα. Ένας άλλος τρόπος εξακρίβωσης της ταυτότητας, περιλαμβάνει την εξέταση διάφορων βιομετρικών χαρακτηριστικών του χρήστη, όπως είναι τα δακτυλικά αποτυπώματα. Ο συνδυασμός πολλαπλών τεχνολογιών εξακρίβωσης της ταυτότητας, έχει ως αποτέλεσμα ισχυρότερη αυθεντικοποίηση.

Διαχείριση συνθηματικών

Τα συνθηματικά είναι ο πιο διαδεδομένος τρόπος για την επιβεβαίωση της ταυτότητας ενός χρήστη. Η ομάδα ασφάλειας του έργου θα εφαρμόσει σύστημα διαχείρισης συνθηματικών, το οποίο εξασφαλίζει τη χρήση ποιοτικών συνθηματικών από τους τελικούς χρήστες του πληροφοριακού συστήματος.

Το σύστημα διαχείρισης συνθηματικών:

- Επιβάλει τη χρήση ατομικών συνθηματικών ώστε να μπορεί να γίνει συσχέτιση των εργασιών στο σύστημα με τους συγκεκριμένους χρήστες.
- Όπου είναι κατάλληλο, επιτρέπει στους χρήστες να επιλέγουν το προσωπικό τους συνθηματικό.
- Επιβάλει τη χρήση ποιοτικών συνθηματικών, κατάλληλων για την κάλυψη των αναγκών του έργου.
- Επιβάλει την τακτική αλλαγή των συνθηματικών
- Επιβάλει την αλλαγή των προσωρινών συνθηματικών κατά την πρώτη είσοδο του χρήστη στο σύστημα.
- Τηρεί ιστορικό των συνθηματικών που χρησιμοποιεί ο κάθε χρήστης για την αποτροπή ανακύκλωσης της χρήσης τους μέσα σε καθορισμένο χρονικό διάστημα.
- Μην εμφανίζει τα συνθηματικά στην οθόνη κατά την εισαγωγή τους.
- Φυλάσσει τα συνθηματικά ξεχωριστά από τα δεδομένα των εφαρμογών και με τρόπο ασφαλή, ενδεχομένως με χρήση μονόδρομης κρυπτογράφησης.
- Αλλάζει τα προκαθορισμένα συνθηματικά που χρησιμοποιούνται από τους κατασκευαστές κατά την εγκατάσταση εφαρμογών στο σύστημα.

Χρήση εργαλείων συστήματος

Τα περισσότερα υπολογιστικά συστήματα διαθέτουν ένα ή περισσότερα ειδικά εργαλεία (system utilities), τα οποία μπορούν να παρακάμπτουν μηχανισμούς ελέγχου του ίδιου του συστήματος ή των εφαρμογών. Είναι απαραίτητο η χρήση τους να είναι περιορισμένη και αυστηρά ελεγχόμενη. Θα πρέπει να εξεταστούν οι ακόλουθοι μηχανισμοί:

- Η χρήση διαδικασιών αυθεντικοποίησης για τα εργαλεία του συστήματος.
- Διαχωρισμός των εργαλείων αυτών από τις υπόλοιπες εφαρμογές.
- Περιορισμός της χρήσης τους από ένα μικρό αριθμό έμπιστων χρηστών.
- Ειδική εξουσιοδότηση για τη χρήση τέτοιων εργαλείων.
- Περιορισμός της διαθεσιμότητας των εργαλείων συστήματος (π.χ. μόνο κατά τη διάρκεια απαραίτητων μεταβολών στο σύστημα).
- Καταγραφή της χρήσης των εργαλείων του συστήματος.
- Καθορισμός των επιπέδων εξουσιοδότησης για τη χρήση τους.
- Απομάκρυνση των μη απαραίτητων εργαλείων από το σύστημα.
- Time-out τερματικών

Περιορισμός χρόνου σύνδεσης

Για εφαρμογές που χαρακτηρίζονται ευαίσθητες για το έργο, επιβάλλεται χρονικό όριο στη σύνδεση του χρήστη με αυτές. Με τον περιορισμό της χρονικής περιόδου κατά την οποία τα τερματικά μπορούν να έχουν πρόσβαση στις υπηρεσίες του συστήματος, περιορίζονται σημαντικά οι ευκαιρίες των μη εξουσιοδοτημένων χρηστών για να αποκτήσουν πρόσβαση στο σύστημα. Τέτοιοι μηχανισμοί είναι απαραίτητοι για όλες τις

κρίσιμες εφαρμογές, ειδικά αυτές που έχουν τερματικά σε χώρους υψηλού κινδύνου. Ο μηχανισμός περιλαμβάνει:

- Τη χρήση προκαθορισμένων χρονικών περιόδων μέσα στα πλαίσια των οποίων θα πρέπει να ολοκληρωθεί κάποια εργασία.
- Τον περιορισμό των δυνατοτήτων σύνδεσης στο σύστημα μόνο σε συγκεκριμένες ώρες (π.χ. κατά το ωράριο εργασίας).

Έλεγχος Πρόσβασης

Κάθε χρήστης του δικτύου θα έχει κάποια καθορισμένα δικαιώματα τα οποία θα του επιτρέπουν τη χρήση των πόρων του δικτύου και των πληροφοριών ανάλογα με τη θέση που έχει και το τμήμα του έργου στο οποίο ανήκει. Τα δικαιώματα αυτά καθορίζονται από τον διαχειριστή του συστήματος σε συνεργασία με τη διοίκηση του φορέα. Ο χρήστης θα πρέπει να συμπληρώσει μια αίτηση στην οποία θα αναγράφονται τα στοιχεία του. Επίσης θα ζητάει τα δικαιώματα που θέλει να του χορηγηθούν για τη χρήση του δικτύου. Στη συνέχεια η αίτηση αυτή θα πηγαίνει στον διαχειριστή του συστήματος ο οποίος θα την μελετά και θα την εγκρίνει η θα την απορρίπτει ανάλογα με το πόσο συμβαδίζουν τα δικαιώματα που ζήτησε ο χρήστης και η δουλειά που κάνει στο έργο.

Πολιτική Ελέγχου Πρόσβασης

Τα δικαιώματα που θα παραχωρηθούν στον κάθε χρήστη εξαρτώνται από τη χρήση του δικτύου που χρειάζεται να κάνει.

Διαχείριση της πρόσβασης των χρηστών.

Όταν ο χρήστης συμπληρώσει την αίτηση απόκτησης δικαιωμάτων και εγκριθεί από τον διαχειριστή του συστήματος δημιουργείται ένας λογαριασμός για το χρήστη που έκανε την αίτηση ο οποίος είναι μοναδικός. Με αυτό το λογαριασμό ο χρήστης καταγράφεται στο σύστημα και παρακολουθούνται όλες του οι ενέργειες. Κάθε ενέργεια του χρήστη καταγράφεται από το σύστημα. Αυτό έχει ως αποτέλεσμα να ελέγχεται διαρκώς η παραβίαση ή μη των δικαιωμάτων που του έχουν παραχωρηθεί από το σύστημα.

Οι λογαριασμοί των χρηστών που δημιουργούνται από το σύστημα πρέπει να είναι μοναδικοί. Γι’ αυτό το λόγο θα ελέγχονται τακτικά από το σύστημα. Επίσης θα υπάρχει ο ίδιος έλεγχος και κατά τη δημιουργία νέων χρηστών.

Για την παραχώρηση προνομιακών δικαιωμάτων σε κάποιο χρήστη απαιτείται μια συμπληρωματική αίτηση που θα υποβάλλεται από τον ίδιο. Σε αυτή την αίτηση ο εν λόγω χρήστης περιγράφει με σαφήνεια τις ενέργειες που χρειάζεται να κάνει στο σύστημα καθώς και το χρόνο που χρειάζεται για να τις φέρει εις πέρας. Κατόπιν ο διαχειριστής του συστήματος εξετάζει την αίτηση και αποφασίζει για την παροχή των προνομιακών δικαιωμάτων. Μόλις ο χρήστης ολοκληρώσει την εργασία του στο σύστημα τα προνομιακά δικαιώματα αφαιρούνται από αυτόν και συνεχίζει κανονικά τη δουλειά του.

Όπως προαναφέρθηκε κάθε χρήστης έχει ένα μοναδικό λογαριασμό για να συνδέεται στο σύστημα. Κάθε λογαριασμός περιέχει έναν κωδικό πρόσβασης (password) ο οποίος είναι και αυτός μοναδικός. Ο χρήστης χρησιμοποιεί τον δικό του κωδικό για να συνδεθεί στο σύστημα. Ο κωδικός αυτός πρέπει να απομνημονευθεί από το χρήστη και να μην είναι γραμμένος σε κάποιο σημείο που μπορεί να το δει οποιοσδήποτε άλλος. Αν για κάποιο λόγο ο χρήστης ξεχάσει τον κωδικό του τότε θα πρέπει να του δοθεί ένας άλλος προσωρινός. Οι προσωρινοί κωδικοί θα υπάρχουν στο σύστημα ως εφεδρικοί και θα χρησιμοποιούνται για τέτοιες περιπτώσεις. Όταν χρησιμοποιηθεί κάποιος από τους προσωρινούς κωδικούς στη συνέχεια θα αλλάζει άμεσα η θα διαγράφεται.

Έλεγχος Πρόσβασης δικτύου (network access control)

Όταν ο χρήστης συμπληρώνει την αίτηση για την απόκτηση λογαριασμού στο σύστημα, τα δικαιώματα που του παραχωρούνται περιλαμβάνουν και την χρήση του δικτύου. Κάθε χρήστης έχει συγκεκριμένη πρόσβαση στους πόρους του δικτύου του έργου. Το τείχος προστασίας απορρίπτει μη εξουσιοδοτημένους χρήστες που προσπαθούν να χρησιμοποιήσουν το δίκτυο της εταιρίας. Αυτό μπορεί να επιτευχθεί με τη χρήση συγκεκριμένων πυλών στο δίκτυο οι οποίες επιτρέπουν στο χρήστη να κινηθεί στο δίκτυο μέχρι το σημείο που του ορίζουν τα δικαιώματά του.

Για τη λειτουργία των εφαρμογών της απαιτείται η χρήση κάποιων θυρών. Οι θύρες αυτές διαχειρίζονται από το τείχος προστασίας.

Άλλες ενέργειες που σχετίζονται με το δίκτυο όπως για παράδειγμα το ηλεκτρονικό ταχυδρομείο (e-mail) ελέγχονται και καταγράφονται από το σύστημα. Όλα τα μηνύματα που εισέρχονται στο σύστημα και εξέρχονται από αυτό ελέγχονται για την ύπαρξη ιών. Επίσης για την μεταφορά αρχείων υπάρχει ο απαιτούμενος έλεγχος. Το σύστημα ελέγχει τα δικαιώματα του κάθε χρήστη και ανάλογα του επιτρέπει να μετακινήσει αρχεία από και προς το σύστημα. Ακόμα από το σύστημα ελέγχεται και καταγράφεται η ώρα και η ημερομηνία κατά την οποία έγιναν οι προαναφερθείσες ενέργειες.

Έλεγχος πρόσβασης στο λειτουργικό σύστημα

Κάθε χρήστης, όπως προαναφέρθηκε, για τη σύνδεσή του στο λειτουργικό σύστημα έχει κάποιον κωδικό πρόσβασης. Το σύστημα ελέγχει και καταγράφει το όνομα του χρήστη και του τερματικού από το οποίο συνδέεται. Επίσης καταγράφει τις επιτυχείς η ανεπιτυχείς προσπάθειες σύνδεσης του κάθε χρήστη με βάση την ημερομηνία και ώρα που έγιναν αυτές. Ο server που έχει το ρόλο του domain controller διαθέτει τους απαραίτητους μηχανισμούς για τον έλεγχο των χρηστών και των τερματικών που συνδέονται στο σύστημα.

Στον server που έχει το ρόλο του domain controller υπάρχουν κάποια εργαλεία του συστήματος όπως για παράδειγμα οι μηχανισμοί που ελέγχουν το domain και άλλοι μηχανισμοί ασφαλείας στα οποία πρόσβαση έχει μόνο ο διαχειριστής του συστήματος. Στα συγκεκριμένα εργαλεία δεν υπάρχει πρόσβαση από μη εξουσιοδοτημένους χρήστες οι οποίοι απορρίπτονται από το σύστημα σε πιθανή προσπάθειά τους σύνδεσης σε αυτό.

Αν κάποιος απομακρυσμένος χρήστης συνδεθεί σε σύστημα του έργου για να πραγματοποιήσει την εργασία του και παραμείνει ανενεργός για ένα μεγάλο χρονικό διάστημα τότε το σύστημα σταματάει τη σύνδεση με αυτό και ο χρήστης θα πρέπει να επανασυνδεθεί. Κάτι αντίστοιχο συμβαίνει και με τη σύνδεση στο internet. Υπάρχει περιορισμός στη χρήση του για την αποτροπή πιθανών κινδύνων που προκύπτουν από αυτή.

Έλεγχος πρόσβασης στις εφαρμογές

Από την ίδια την εφαρμογή δίνεται η δυνατότητα δημιουργίας ρόλων των χρηστών στους οποίους καθορίζονται σαφώς τα δικαιώματα χρήσης της. Ως επί το πλείστο τα μέλη της ομάδας έργου έχουν πρόσβαση με ένα μεγάλο μέρος των εφαρμογών για να μπορούν να κάνουν τις δοκιμές και τις αναβαθμίσεις σε αυτήν καθώς επίσης να μπορούν να υποστηρίξουν τους χρήστες που τη χρησιμοποιούν. Οι απομακρυσμένοι χρήστες δεν έχουν όμως τα ίδια δικαιώματα. Τα δικαιώματα που τους χορηγούνται περιλαμβάνουν αυστηρά κάποια τμήματα των εφαρμογών και μόνο σε αυτά είναι δυνατή η πρόσβαση.

Τα μηχανήματα στα βρίσκονται και δουλεύουν οι εφαρμογές (servers) είναι τοποθετημένα σε χώρο που δεν υπάρχει πρόσβαση από κανένα παρά μόνο από το

διαχειριστή του συστήματος. Η πρόσβαση στο χώρο που βρίσκεται ο διαχειριστής του συστήματος καθώς και σε αυτόν που βρίσκονται τα μηχανήματα ελέγχεται με κάρτες ασφαλείας.

Παρακολούθηση προσπέλασης και χρήσης συστήματος

Τα συστήματα έχουν τη δυνατότητα να καταγράφει και να παρακολουθεί κάθε ενέργεια που γίνεται από τους χρήστες πάνω σε αυτό. Κάθε σύστημα παρακολουθείται τακτικά από τον διαχειριστή ο οποίος ελέγχει τις κινήσεις των χρηστών καθώς επίσης και την τήρηση των δικαιωμάτων που τους παραχωρήθηκαν.

Η καταγραφή όλων των γεγονότων πρέπει να γίνεται από το σύστημα σε συγκεκριμένα αρχεία (audit logs).

Όπως προαναφέρθηκε ο διαχειριστής του συστήματος ελέγχει όλες τις κινήσεις που γίνονται από τους χρήστες στο δίκτυο. Αυτό γίνεται με τη βοήθεια ειδικών μηχανισμών που υπάρχουν στον server που είναι ο domain controller. Με τη χρήση των μηχανισμών αυτών καταγράφεται το όνομα του χρήστη, το τερματικό που χρησιμοποίησε, τα προγράμματα που χρησιμοποίησε καθώς και η ώρα και η ημερομηνία που συνδέθηκε και αποσυνδέθηκε από αυτό. Επίσης καταγράφεται αν ο χρήστης έχει προνομιακά δικαιώματα και οι προσπάθειες μη εξουσιοδοτημένης πρόσβασης (η παραβίαση των δικαιωμάτων που του έχουν παραχωρηθεί δηλαδή). Τα αρχεία αυτά όπως αναφέρθηκε πιο πάνω ελέγχονται αρκετά συχνά από το διαχειριστή του συστήματος ο οποίος είναι ο μοναδικός που έχει πρόσβαση σε αυτά. Τα μηχανήματα στα οποία φυλάσσονται τα log αρχεία ελέγχονται από ένα πρόγραμμα που συγχρονίζει τα ρολόγια τους. Έχουν δηλαδή όλα την ίδια ώρα και συμβαδίζουν με την τοπική.

Έλεγχος της πρόσβασης στις εφαρμογές

Σκοπός είναι η αποτροπή της μη εξουσιοδοτημένης πρόσβασης στις πληροφορίες που βρίσκονται στα συστήματα. Σύμφωνα με την πολιτική ασφάλειας, οι εφαρμογές:

- Ελέγχουν την πρόσβαση του χρήστη σε διάφορες λειτουργίες και δεδομένα, σύμφωνα με την πολιτική ασφάλειας του έργου.
- Παρέχουν προστασία από μη εξουσιοδοτημένη πρόσβαση για χρήση λειτουργιών του λειτουργικού συστήματος, ικανών να παρακάμψουν τους μηχανισμούς ασφάλειας και ελέγχου.
- Προστατεύουν και την ασφάλεια άλλων συστημάτων, με τα οποία διαμοιράζονται δεδομένα.
- Παρέχουν πρόσβαση στα δεδομένα του συστήματος μόνο στους εξουσιοδοτημένους χρήστες ή ομάδες χρηστών.

Περιορισμοί πρόσβασης στις πληροφορίες

Τα δικαιώματα προσπέλασης των χρηστών των εφαρμογών του συστήματος, ορίζονται από την πολιτική ασφάλειας του έργου. Επ’ αυτού, θα πρέπει επίσης να λαμβάνονται υπόψη οι ανάγκες όλων των ομάδων των χρηστών του συστήματος (προσωπικό, εξωτερικοί συνεργάτες, προσωπικό υποστήριξης κλπ.), όπως και οι επιχειρησιακές ανάγκες του έργου. Στην κατεύθυνση αυτή, μπορούν να χρησιμεύσουν οι ακόλουθοι μηχανισμοί:

- Η χρήση μενού επιλογών μέσω των οποίων θα ελέγχεται και θα κατευθύνεται η χρήση των εφαρμογών.
- Ο περιορισμός των γνώσεων των χρηστών για τις εφαρμογές του συστήματος, στα απολύτως απαραίτητα για την εργασία τους.
- Ο έλεγχος των δικαιωμάτων πρόσβασης των χρηστών.

- Η διασφάλιση του ότι τα παράγωγα εφαρμογών που χειρίζονται ευαίσθητα δεδομένα (εκτυπώσεις, αρχεία κλπ.) κατευθύνονται μόνο στα κατάλληλα προστατευμένα και διαβαθμισμένα τερματικά.

Καταγραφή γεγονότων

Στο σύστημα τηρούνται αρχεία που καταγράφουν κάθε συμβάν σχετικό με την ασφάλεια κάθε συστήματος. Τα αρχεία αυτά (audit logs) φυλάσσονται για συγκεκριμένο χρονικό διάστημα ώστε να είναι δυνατή η χρησιμοποίηση τους σε ενδεχόμενες έρευνες. Περιλαμβάνουν τα ακόλουθα:

- Την ταυτότητα των χρηστών (user IDs).
- Τον ακριβή χρόνο σύνδεσης και αποσύνδεσης του χρήστη.
- Το τερματικό το οποίο χρησιμοποιεί ο χρήστης.
- Τις επιτυχείς αλλά και τις ανεπιτυχείς προσπάθειες του χρήστη να προσπελάσει το σύστημα.
- Τις επιτυχείς και τις ανεπιτυχείς προσπάθειες του χρήστη να προσπελάσει δεδομένα του συστήματος.

Καταγραφή της χρήσης του συστήματος

Στη διαδικασία αυτή παρακολουθείται η χρήση κάθε συστήματος. Συγκεκριμένα θα παρακολουθούνται:

- Η εξουσιοδοτημένη πρόσβαση (χρήστης, ώρα, τύπος πρόσβασης, πόροι που προσπελάσθηκαν, προγράμματα που χρησιμοποιήθηκαν).
- Η χρήση ειδικών προνομίων στο σύστημα (χρήση προνομιακών συνθηματικών χρηστών, έναρξη και τερματισμός λειτουργίας του συστήματος, χρήση εξωτερικών συσκευών).
- Οι προσπάθειες μη εξουσιοδοτημένης πρόσβασης (αποτυχημένες προσπάθειες, μηνύματα από ηλεκτρονικές πύλες ασφαλείας ή συστήματα ανίχνευσης επιθέσεων - intrusion detection).
- Μηνύματα του συστήματος (μηνύματα λάθους, μηνύματα δικτύου κλπ.).

Συγχρονισμός των συστημάτων

Η σωστή ρύθμιση των ρολογιών των υπολογιστών είναι ιδιαίτερα σημαντική για την ακρίβεια των περιεχομένων των αρχείων καταγραφής, ειδικά όταν πρόκειται να χρησιμοποιηθούν ως αποδεικτικά στοιχεία σε κάποια έρευνα. Όταν κάποια συσκευή διαθέτει ρολόι πραγματικού χρόνου, αυτό θα πρέπει να ρυθμιστεί σύμφωνα με κάποιο συγκεκριμένο πρότυπο (για παράδειγμα το Universal Coordinated Time, UCT) ή την τοπική ώρα. Εφόσον κάποια τέτοια ρολόγια δεν είναι ιδιαίτερα ακριβή, θα πρέπει να υπάρχει κάποια διαδικασία ελέγχου και διόρθωσης της ώρας που δείχνουν.

Διαχείριση Επιχειρησιακής Συνέχειας

Σκοπός είναι η αποτροπή παρεμβολών στις επιχειρηματικές δραστηριότητες του έργου και η προστασία των κρίσιμων διαδικασιών στην περίπτωση μερικών ή ολικών καταστροφών.

Μέθοδος

Παράμετροι της διαχείρισης της επιχειρησιακής συνέχειας

Η διαδικασία διαχείρισης της επιχειρησιακής συνέχειας του έργου (business continuity management process) χρησιμοποιείται για τη μείωση σε κάποιο ανεκτό επίπεδο των επιπτώσεων από καταστροφές και συμβάντα σχετικά με την ασφάλεια των πληροφοριών του έργου.

Διαδικασία διαχείρισης της επιχειρησιακής συνέχειας

Ο Υπεύθυνος Ασφάλειας του έργου, σύμφωνα με την πολιτική ασφάλειας, έχει καθιερώσει συγκεκριμένη διαδικασία για το σχεδιασμό και την υλοποίηση της επιχειρησιακής συνέχειας.

Συγκεκριμένα, βασίζεται στα ακόλουθα:

- στην κατανόηση των κινδύνων που ενδέχεται να απειλούν το έργο, την πιθανότητα να υλοποιηθούν και το κόστος που θα επιφέρουν.
- στην κατανόηση των επιπτώσεων κάθε παρεμβολής στη φυσιολογική λειτουργία του έργου.
- στην κατάστρωση μιας στρατηγικής επιχειρησιακής συνέχειας η οποία θα πρέπει να είναι σύμφωνη με τους στόχους και τις προτεραιότητες του οργανισμού.
- στην καταγραφή ενός σχεδίου επιχειρησιακής συνέχειας το οποίο θα υλοποιεί την παραπάνω στρατηγική.
- στον τακτικό έλεγχο και την τακτική ενημέρωση του σχεδίου και των διαδικασιών που προβλέπονται σε αυτό.
- στην ενσωμάτωση του σχεδίου επιχειρησιακής συνέχειας σε όλες τις λειτουργίες του έργου. Η ευθύνη της υλοποίησης του σχεδίου βρίσκεται στην ομάδα ασφάλειας του έργου.

<u>Διαχείριση Ασφάλειας</u>

Η διαχείριση της ασφάλειας έχει ως γενικό σκοπό την τήρηση των διαχειριστικών ασφαλιστικών μεθόδων σχετικά με την «υποδομή της ασφάλειας πληροφοριών» και την «ασφάλεια προσπέλασης τρίτων μερών».

Η ***υποδομή της ασφάλειας πληροφοριών*** έχει ως σκοπό και αντικείμενο τη διαχείριση της ασφάλειας μέσα στο έργο. Επ' αυτού έχει δημιουργηθεί ένα πλαίσιο διαχείρισης προκειμένου να ελέγχεται η υλοποίηση της ασφάλειας των πληροφοριών μέσα στην ομάδα έργου. Για την εκπλήρωση του σκοπού, θα πρέπει να υπάρχει έμπρακτο ενδιαφέρον και υποστήριξη από τη διοίκηση του έργου για τη δημιουργία της πολιτικής ασφάλειας, τον καταμερισμό καθηκόντων και τη μεθοδική εφαρμογή της τελευταίας στο έργο. Για την εκπλήρωση και ακριβή υλοποίηση του σκοπού, θα πρέπει να επιδιωχθεί η συνεργασία διαφορετικών ομάδων, όπως οι χρήστες, τα στελέχη των εμπλεκομένων τμημάτων και η διοίκηση του έργου.

<u>Έλεγχος Συμμόρφωσης</u>

Σκοπός είναι η αποφυγή παραβίασης νόμων, ρυθμίσεων ή συμβάσεων, η διασφάλιση της συμμόρφωσης των συστημάτων με την πολιτική ασφάλειας του έργου καθώς και η μεγιστοποίηση της αποτελεσματικότητας της διαδικασίας ελέγχου κάθε

πληροφοριακού συστήματος με ταυτόχρονη ελαχιστοποίηση των παρεμβολών από ή προς αυτό.

Μέθοδος

Καθορισμός της σχετικής νομοθεσίας

Όλες οι υποχρεώσεις που απορρέουν από τη σχετική νομοθεσία θα πρέπει να είναι καταγεγραμμένες για κάθε σύστημα. Επιπλέον θα πρέπει να ορίζονται οι υπεύθυνοι και οι μηχανισμοί συμμόρφωσης.

Πνευματική ιδιοκτησία

Copyright

Η ομάδα ασφάλειας του έργου θα πρέπει να λαμβάνει τα κατάλληλα μέτρα για τη συμμόρφωση με τις υποχρεώσεις που προκύπτουν από δικαιώματα δημιουργών, σχεδιαστών ή τη χρήση ονομάτων. Η παραβίαση τέτοιων δικαιωμάτων μπορεί να οδηγήσει σε νομικές κυρώσεις.

Copyright λογισμικού

Το λογισμικό παρέχεται με βάση άδεια χρήσης, η οποία και περιορίζει την εγκατάσταση ή τη χρήση του λογισμικού σε συγκεκριμένους υπολογιστές ή από συγκεκριμένο αριθμό χρηστών. Έπ' αυτού, θα εξετάζονται τα ακόλουθα ζητήματα:

- Η δημιουργία πολιτικής για τη συμμόρφωση με τα πνευματικά δικαιώματα που σχετίζονται με το χρησιμοποιούμενο από το έργο λογισμικό.
- Η δημιουργία συγκεκριμένης πολιτικής με βάση την οποία θα γίνεται η προμήθεια λογισμικού.
- Η εκπαίδευση και ενημέρωση του προσωπικού στα θέματα πνευματικής ιδιοκτησίας και τις επιπτώσεις τους για το έργο.
- Η δημιουργία και τήρηση αρχείου του χρησιμοποιούμενου λογισμικού.
- Η διατήρηση αποδείξεων για τη νόμιμη χρήση λογισμικού (άδειες χρήσης, πρωτότυπα του λογισμικού κλπ.).
- Η δημιουργία διαδικασίας που να ελέγχει ότι δε χρησιμοποιείται στο έργο παράνομα εγκατεστημένο λογισμικό.
- Η δημιουργία διαδικασίας για την απεγκατάσταση ή μεταφορά λογισμικού σε τρίτους.
- Η συμμόρφωση με τους όρους απόκτησης και χρήσης λογισμικού μέσω δημόσιων δικτύων.

Προστασία των αρχείων του έργου

Όλα τα σημαντικά αρχεία του έργου προστατεύονται απέναντι στο ενδεχόμενο μερικής ή ολικής καταστροφής ή νοθείας. Νομικές διατάξεις επιβάλουν τη τήρηση αρχείων για συγκεκριμένο χρονικό διάστημα. Τέτοια αρχεία μπορεί να χρησιμεύουν ως αποδεικτικά στοιχεία της νόμιμης λειτουργίας του έργου. Τα αρχεία θα πρέπει να είναι κατανεμημένα σε κατηγορίες, π.χ. λογιστικά, διαδικασίες, logs κλπ. Για κάθε κατηγορία θα πρέπει να είναι καθορισμένη η χρονική περίοδος διατήρησης των αρχείων, καθώς και το μέσο φύλαξης. Στην περίπτωση που χρησιμοποιείται κρυπτογραφία για κάποιο αρχείο, τα σχετικά κλειδιά θα πρέπει να φυλάσσονται ξεχωριστά και να είναι διαθέσιμα μόνο στους εξουσιοδοτημένους χρήστες. Θα πρέπει να δοθεί προσοχή στο ενδεχόμενο

φυσικής φθοράς του μέσου αποθήκευσης των αρχείων, το οποίο θα πρέπει να χρησιμοποιείται σύμφωνα με τις οδηγίες του κατασκευαστή. Για τα μαγνητικά μέσα αποθήκευσης θα πρέπει να υπάρχουν και διαδικασίες ελέγχου της σωστής λειτουργίας.

Το σύστημα αποθήκευσης των αρχείων θα πρέπει να μπορεί να αναγνωρίσει και να χειριστεί ανάλογα τις διάφορες κατηγορίες αρχείων καθ' όλο το χρονικό διάστημα τήρησής τους. Θα πρέπει επίσης να μπορεί να τα καταστρέψει κατάλληλα μετά το πέρας της αναγκαιότητας φύλαξής τους.

Η ομάδα ασφάλειας του έργου, θα πρέπει να:

- χρησιμοποιεί τις κατάλληλες διαδικασίες για την αποθήκευση, τη διαχείριση, τον έλεγχο και την καταστροφή των διάφορων τύπων αρχείων.
- έχει καθορισμένο χρονοδιάγραμμα ελέγχου της καταλληλότητας των μέσων αποθήκευσης των αρχείων.
- καθορίσει αναλυτικά τις πληροφορίες που θα αποθηκεύει.
- χρησιμοποιεί τους κατάλληλους μηχανισμούς προστασίας των αρχείων.

Προστασία δεδομένων και προστασία πληροφοριών προσωπικού χαρακτήρα

Για τη διαδικασία αυτή, η ομάδα ασφάλειας συμβουλεύει τα μέλη της ομάδας έργου για τις ευθύνες τους, τις διαδικασίες και τον τρόπο διαχείρισης προσωπικών δεδομένων. Οι υπεύθυνοι ασφάλειας και προστασίας των δεδομένων θα πρέπει να είναι ενήμεροι για όλα τα αρχεία προσωπικού χαρακτήρα που τηρούνται στα πλαίσια του έργου ώστε να διασφαλίσουν τη συμμόρφωσή τους με την υπάρχουσα νομοθεσία.

Πρόληψη κατάχρησης του πληροφοριακού συστήματος

Κάθε πληροφοριακό σύστημα του έργου θα πρέπει να χρησιμοποιείται αποκλειστικά για τις λειτουργικές ανάγκες του έργου. Η διοίκηση έργου θα πρέπει να εξουσιοδοτεί τους εμπλεκόμενους στη χρήση του. Οποιαδήποτε χρήση του συστήματος για σκοπούς που δεν έχουν σχέση με το έργο, χωρίς την προηγούμενη εξουσιοδότηση της διοίκησης, θα πρέπει να χαρακτηρίζεται ως κατάχρηση. Αν κάποια τέτοια δραστηριότητα γίνει αντιληπτή με οποιοδήποτε τρόπο, θα πρέπει να γνωστοποιηθεί στη διοίκηση, η οποία είναι υπεύθυνη για την επιβολή κατάλληλων κυρώσεων.

Η διοίκηση του έργου, θα πρέπει να δίνει στο προσωπικό – χρήστες του συστήματος γραπτή εξουσιοδότηση με συγκεκριμένα δικαιώματα σε αυτό.

Επιπλέον οι χρήστες θα πρέπει να υπογράφουν ότι έλαβαν γνώση των δικαιωμάτων τους. Όλοι οι χρήστες του συστήματος, προσωπικό και εξωτερικοί συνεργάτες, θα πρέπει να ενημερώνονται για τις συνέπειες της κατάχρησής του. Κατά τη διαδικασία της σύνδεσης στο σύστημα θα πρέπει να εμφανίζεται σχετικό προειδοποιητικό μήνυμα. Ο χρήστης θα πρέπει να επιβεβαιώσει ότι έλαβε γνώση του μηνύματος πριν συνεχίσει την εργασία του στο αντίστοιχο πληροφοριακό σύστημα.

Μέτρα ασφάλειας για τις εγκαταστάσεις και το προσωπικό του Αναδόχου

Η Neuropublic ΑΕ εφαρμόζει Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) πιστοποιημένο κατά ISO27001. Στο πλαίσιο της συμμόρφωσης με το πρότυπο ISO27001 η Neuropublic ΑΕ εφαρμόζει ένα ολοκληρωμένο σύνολο οργανωτικών και τεχνικών μέτρων ασφάλειας και προστασίας δεδομένων, οριζόντια για το σύνολο των συστημάτων που διαθέτει, φιλοξενεί, ή διαχειρίζεται. Ειδικότερα, αναφέρουμε τα παρακάτω μέτρα.

Έλεγχος λογικής πρόσβασης

Η NEUROPUBLIC εφαρμόζει ολοκληρωμένο σύστημα εγγραφής, ταυτοποίησης και αυθεντικοποίησης χρηστών, απονομής δικαιωμάτων, ελέγχου λογικής πρόσβασης, λογιστικής παρακολούθησης της εισόδου στα συστήματα και των ενεργειών σε επίπεδο συστήματος (system/audit log). Υλοποιεί αυστηρή πολιτική ελέγχου πρόσβασης μέσω του Active Directory, έλεγχο χρήσης των σταθμών εργασίας (π.χ. απαγόρευση χρήσης usb συσκευών) μέσω λογισμικού Endpoint Security, έλεγχο δικτυακής πρόσβασης μέσω firewall (διάταξη DMZ με χρήση δύο firewalls για το διαχωρισμό των υποδικτύων).

Ενημέρωση και συμμόρφωση προσωπικού

Η Neuropublic ΑΕ διασφαλίζει ότι το προσωπικό το οποίο διαχειρίζεται δεδομένα προσωπικού χαρακτήρα και, γενικότερα, εμπιστευτικά δεδομένα έχει αποδεχθεί στο πλαίσιο της σύμβασής του με τη NEUROPUBLIC σχετική «ρήτρα εμπιστευτικότητας» και έχει λάβει γνώση των πολιτικών ασφάλειας και προστασίας δεδομένων.

Κρυπτογράφηση δεδομένων

Η Neuropublic ΑΕ εφαρμόζει το πρωτόκολλο TLS, στην νεότερή του έκδοση, για την κρυπτογράφηση της διαδικτυακής επικοινωνίας σε όλα τα συστήματά της που είναι προσβάσιμα μέσω Διαδικτύου. Επιπλέον, εφαρμόζεται VPN για την πρόσβαση στα συστήματα των πελατών της.

Εμπιστευτικότητα δεδομένων και πνευματικά δικαιώματα

Η Neuropublic προστατεύει τα δεδομένα προσωπικού χαρακτήρα, καθώς και τα δεδομένα των οποίων τα πνευματικά δικαιώματα προστατεύονται και ιδιαιτέρως εκείνων που τα πνευματικά δικαιώματα ανήκουν σε τρίτους, εφαρμόζοντας:

- Ολοκληρωμένο σύστημα ελέγχου λογικής πρόσβασης (Active Directory / LDAP),
- Ανάχωμα ασφάλειας (firewall) και αρχιτεκτονική DMZ με δύο ανεξάρτητους firewall,
- Σύστημα ανίχνευσης και αποτροπής παρεισφρήσεων (IDS/IPS),
- Σύστημα προστασίας από κακόβουλο λογισμικό (endpoint security) και ελέγχου χρήσης των σταθμών εργασίας,
- Κρυπτογράφηση των επικοινωνιών,
- Λογιστική καταγραφή και έλεγχο (audit).

Επιπλέον, διασφαλίζει τον περιορισμό της πρόσβασης στα δεδομένα μόνο των στελεχών για τα οποία απαιτείται η πρόσβαση στο πλαίσιο των εργασιών τους (need-to-know), ενημερώνει τα στελέχη της για τις υποχρεώσεις τους έναντι του νόμου, καθώς και για εκείνες που προκύπτουν από τις συμβατικές υποχρεώσεις της NEUROPUBLIC και την εφαρμογή της πολιτικής ασφάλειας και προστασίας της ιδιωτικότητας. Η NEUROPUBLIC έχει εκπονήσει ανάλυση επικινδυνότητας, σύμφωνα με τα οριζόμενα στο ISO27001, ώστε να διασφαλίσει ότι τα μέτρα ασφάλειας που εφαρμόζει εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων.