ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΝΑΥΤΙΛΙΑΣ
ΚΑΙ ΝΗΣΙΩΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ
ΑΡΧΗΓΕΙΟ ΛΙΜΕΝΙΚΟΥ ΣΩΜΑΤΟΣ
ΕΛΛΗΝΙΚΗΣ ΑΚΤΟΦΥΛΑΚΗΣ
ΚΛΑΔΟΣ ΔΙΟΙΚΗΣΗΣ &
ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΗΣ
ΔΙΑΚΥΒΕΡΝΗΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ Γ΄
Ταχ. Δ/νση : Ακτή Βασιλειάδη Πύλη Ε2
Ταχ. Κώδικας : 18510, Πειραιάς
Τηλέφωνο : 213 137 1761
FAX : 210 452 2630
Email : didep.c@hcg.gr

Πειραιάς, 24-03-2020
Αριθ. πρωτ.: 2433.4/19880/2020

ΠΡΟΣ: Ως Πίνακα Αποδεκτών

ΘΕΜΑ: «Εγκύκλιος Πολιτικής Ασφαλείας Πληροφοριακών Συστημάτων του Υ.ΝΑ.Ν.Π.»

ΣΧΕΤ. : α) Το Π.Δ. 13/2018 «Οργανισμός Υπουργείου Ναυτιλίας και Νησιωτικής Πολιτικής» (Α' 26), όπως έχει τροποποιηθεί και ισχύει.

β) Ν. 4577/2018 (Α΄ 199) «Ενσωμάτωση Οδηγίας 2016/1148/ΕΕ σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις - γνωστή ως Οδηγία NIS».

γ) Ν. 4624/2019 (Α΄ 137) «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 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 ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις».

δ) Η αριθμ. 1027 Υ.Α. (Β΄ 3739/08-10-19) με θέμα «Θέματα εφαρμογής και διαδικασιών του ν. 4577/2018 (Α΄ 199)».

1. Γνωρίζεται ότι σύμφωνα με το άρθρο 33 του (α) σχετικού, η Διεύθυνση Ηλεκτρονικής Διακυβέρνησης και Επικοινωνιών (Δ.Η.Δ.ΕΠ.) του ΑΛΣ-ΕΛ.ΑΚΤ., είναι μεταξύ άλλων αρμόδια για την ανάπτυξη και εφαρμογή της πολιτικής ασφαλείας των πληροφοριακών συστημάτων του Φορέα μας. Με την πολιτική ασφαλείας καθορίζεται ένα ελάχιστο βασικό επίπεδο ασφαλείας των πληροφοριακών συστημάτων όχι μόνο σε ότι αφορά την κεντρική υποδομή του Φορέα αλλά περιλαμβάνει και τα συστήματα - υποδομή που χρησιμοποιούνται από τους χρήστες ήτοι τα στελέχη του κατά την ενάσκηση των καθημερινών καθηκόντων τους, με απώτερο τελικό σκοπό την εξασφάλιση της προστασίας από κάθε είδους απειλή, τυχαία ή σκόπιμη.

2. Η προαναφερόμενη Πολιτική Ασφαλείας κατόπιν ολοκλήρωσης της ανάπτυξης και επεξεργασίας της από την επισπεύδουσα Υπηρεσία επισυνάπτεται στο παρόν στην τελική της μορφή. Το πεδίο εφαρμογής

της εν λόγω εγκυκλίου αφορά το σύνολο των στελεχών και Υπηρεσιών του Φορέα, όπως αναφέρεται αναλυτικά στο αντίστοιχο κεφάλαιο αυτής.

3. Της παρούσης να λάβει γνώση το σύνολο των στελεχών (ένστολο και πολιτικό προσωπικό) του Φορέα, με την επίδειξη της δέουσας υπευθυνότητας, επιμέλειας και συνέπειας ως προς την τήρηση των μέτρων ασφαλείας πληροφοριακών συστημάτων που περιγράφονται.-

Ο ΥΠΟΥΡΓΟΣ

Ιωάννης Πλακιωτάκης

Επισυνάπτεται:
Η Πολιτική Ασφαλείας Πληροφοριακών Συστημάτων Υ.ΝΑ.Ν.Π. (σ. 19).

ΠΙΝΑΚΑΣ ΔΙΑΝΟΜΗΣ :

Ι. ΑΠΟΔΕΚΤΕΣ ΓΙΑ ΕΝΕΡΓΕΙΑ :
Γενικό

ΙΙ. ΕΣΩΤΕΡΙΚΗ ΔΙΑΝΟΜΗ :
1. Γρ. κ. Υ.ΝΑ.Ν.Π.
2. Γρ. κ. Γ.Γ.Λ.Λ.Π.Ν.Ε.
3. Γρ. κ. Γ.Γ.ΑΙ.Ν.Π.
4. Γρ. κ. Α/ΛΣ – ΕΛ.ΑΚΤ.
5. Γρ. κ. Α΄Υ/ΛΣ – ΕΛ.ΑΚΤ.
6. Γρ. κ. Β΄Υ/ΛΣ – ΕΛ.ΑΚΤ
7. Γρ. κ. ΓΕΛΣ – ΕΛ.ΑΚΤ
8. Γρ. κ. ΔΚΔ΄
9. Γρ. κ. ΓΔΟΥ

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΕΚΔΟΣΗ 1.0

Δραπετσώνα, Ιανουάριος 2020

Περιεχόμενα

1. Εισαγωγή

1.1. Αναγκαιότητα της πολιτικής ασφάλειας

Οι πληροφορίες, τα δεδομένα, τα συστήματα πληροφορικής και οι μέθοδοι εργασίας αποτελούν βασικά «περιουσιακά στοιχεία» του ΛΣ-ΕΛ.ΑΚΤ. και κατ΄ επέκταση του Υ.ΝΑ.Ν.Π. Οποιαδήποτε έκπτωση στην διαθεσιμότητα, την ακεραιότητα και το απόρρητο των πληροφοριών δημιουργεί σοβαρά προβλήματα στην εύρυθμη λειτουργία των επιχειρησιακών δραστηριοτήτων ενώ η πιθανή απώλεια-διαρροή προσωπικών δεδομένων αντιβαίνει στις διατάξεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR) και ταυτόχρονα βλάπτει την εικόνα και το κύρος του Φορέα. Επιπλέον, η φύση των δραστηριοτήτων του ΛΣ-ΕΛ.ΑΚΤ. υπαγορεύει τη διατήρηση μεγάλου όγκου πληροφοριών που αφορούν τον Φορέα αλλά και προσωπικών στοιχείων (π.χ. σχετικά με στελέχη, πολίτες, κ.ο.κ.) τα οποία υπόκεινται σε διάφορες νομοθετικές διατάξεις και κατά συνέπεια είναι απαραίτητο να είναι ασφαλή από απειλές που μπορούν να προέλθουν από διάφορες πηγές (κυβερνοεπιθέσεις, φυσικές καταστροφές, λάθη χρηστών, απάτη μέσω διαδικτύου, ιοί, υποκλοπή δεδομένων κλπ).

Για τους ανωτέρω λόγους, η ασφάλεια των πληροφοριακών συστημάτων (εφεξής ΠΣ) του ΛΣ-ΕΛ.ΑΚΤ. και Υ.ΝΑ.Ν.Π. είναι ιδιαίτερης σημασίας και ως εκ τούτου επιβάλλεται η διαμόρφωση ενός περιβάλλοντος αυξημένων μέτρων με κύριο στόχο την διατήρηση ικανοποιητικού επιπέδου εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των συστημάτων - δικτύων και κατ' επέκταση των δεδομένων που αυτά επεξεργάζονται.

Η παρούσα πολιτική ασφάλειας (εφεξής ΠΑ) καθορίζει τους κανόνες, σύμφωνα με τους οποίους τα ΠΣ πρέπει να σχεδιάζονται, να εγκαθίστανται, να λειτουργούν και να συντηρούνται και διαμορφώνει συγκεκριμένες διαδικασίες, μέσα από τις οποίες επιτυγχάνεται η μεγιστοποίηση της ασφάλειας των ΠΣ ενώ ταυτόχρονα θέτει και τις βασικές αρχές οι οποίες πρέπει να τηρούνται από τους χρήστες – στελέχη του Φορέα. Η ΠΑ καθώς και οι διαδικασίες που την υποστηρίζουν οφείλουν να αναθεωρούνται σε τακτική βάση προκειμένου να προσαρμόζονται στις νέες καταστάσεις, κινδύνους και περιορισμούς.

1.2. Βασικές Αρχές και Στόχοι της ΠΑ

Οι βασικοί στόχοι της ΠΑ είναι οι ακόλουθοι:

- **Η εξασφάλιση της αρχής της εμπιστευτικότητας (Confidentiality)**: Πρόκειται για την προστασία των πληροφοριών ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίησή τους. Οι πληροφορίες σε έντυπη και ηλεκτρονική μορφή κάτω από συγκεκριμένες συνθήκες δύνανται να παραβιαστούν και να αναγνωστούν από τρίτους.

- **Η εξασφάλιση της αρχής της ακεραιότητας (Integrity):** Αφορά στην προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους.

- **Η εξασφάλιση της αρχής της διαθεσιμότητας (Availability):** Τα δεδομένα αντιπροσωπεύουν τα αποτελέσματα της μακροχρόνιας εργασίας των στελεχών και είναι εξίσου σημαντικά τόσο για μεμονωμένους χρήστες όσο και για τον ίδιο τον Φορέα. Είναι σημαντικό να καταβάλλεται κάθε προσπάθεια ώστε αυτά να είναι άμεσα διαθέσιμα προς χρήση και αξιοποίηση.

- Η ικανοποίηση των νομικών και κανονιστικών απαιτήσεων σχετικών με την ασφάλεια και προστασία των ΠΣ.

- Η επιχειρησιακή συνέχεια των βασικών υπηρεσιών του Οργανισμού έναντι περιστατικών παραβίασης της ΠΑ.

- Η ενημέρωση και η εκπαίδευση όλων των χρηστών και λοιπών εμπλεκομένων τρίτων σχετικά με τους κανόνες που τίθενται από την ΠΑ.

- Η άμεση κοινοποίηση και διαχείριση περιστατικών ή αδυναμιών ασφαλείας.

1.3. Δομή της πολιτικής ασφάλειας

Η πολιτική ασφάλειας του ΛΣ-ΕΛ.ΑΚΤ αποτελείται από δύο μέρη:

- **Μέρος Α:** Το πρώτο μέρος παρουσιάζει τις απαραίτητες οργανωτικές δομές και αναλύει τις διαδικασίες που πρέπει να τηρούνται τόσο από άποψη ανθρώπινου δυναμικού, όσο και από άποψη συστημάτων.

- **Μέρος Β:** Το δεύτερο μέρος απαρτίζεται από κεφάλαια καθένα από τα οποία εστιάζει σε ειδικότερες περιοχές - τομείς της ασφάλειας είτε αναλύοντας τα τεχνικά χαρακτηριστικά των διαφορετικών συστημάτων που χρησιμοποιούνται και των παραμέτρων ασφάλειας που πρέπει να ρυθμίζονται είτε περιγράφοντας βασικές αρχές / διαδικασίες και όρους χρήσης που πρέπει να εφαρμόζονται για ζητήματα που άπτονται της καλής χρήσης και της ασφάλειας των ΠΣ από τους τελικούς χρήστες.

1.4. Πεδίο εφαρμογής

Η παρούσα πολιτική έχει εφαρμογή σε όλα τα ΠΣ του ΛΣ-ΕΛ.ΑΚΤ. και κατ΄ επέκταση του Υ.ΝΑ.Ν.Π. Όλο το ένστολο προσωπικό του Λ.Σ.-ΕΛ.ΑΚΤ., οι πολιτικοί υπάλληλοι αλλά και συστήματα - χρήστες άλλων Φορέων - Οργανισμών - Εταιριών εφόσον κάνουν χρήση των συστημάτων - δεδομένων του υποχρεούνται να συμμορφώνονται προς τις απαιτήσεις της παρούσας ΠΑ και να συμβάλουν στην ενίσχυση των πρακτικών ασφαλείας.

ΜΕΡΟΣ Α

2. Οργάνωση Υπηρεσίας

2.1. Γενικά

Στο κεφάλαιο αυτό αναφέρονται οι δομές του Φορέα που σχετίζονται με την πολιτική ασφάλειας του ΛΣ-ΕΛ.ΑΚΤ. Στη συνέχεια, γίνεται σύντομη περιγραφή των αρμοδιοτήτων τους.

2.2. Υφιστάμενες διοικητικές δομές ΑΛΣ-ΕΛΑΚΤ

- **ΔΗΔΕΠ**: Η Διεύθυνση Ηλεκτρονικής Διακυβέρνησης και Επικοινωνιών, σύμφωνα με το Π.Δ. 13/2018(Α΄ 26), όπως ισχύει, είναι αρμόδια μεταξύ άλλων για την ανάπτυξη και την εφαρμογή ΠΑ.

- **Μονάδα Εσωτερικού Ελέγχου (ΜΕΕ) ΛΣ-ΕΛΑΚΤ**: Σύμφωνα με το Π.Δ. 13/2018 (άρθρο 4, παρ. 8) η Μονάδα Εσωτερικού Ελέγχου, ασκεί την αρμοδιότητα του ελέγχου των πληροφοριακών συστημάτων, προκειμένου να διαπιστωθεί κατά πόσον επιτυγχάνουν τους σκοπούς τους και εάν έχουν ενσωματωθεί σε αυτά επαρκείς ασφαλιστικές δικλείδες/μηχανισμοί ελέγχου.

2.3. Εσωτερικές οργανωτικές δομές ασφαλείας ΑΛΣ-ΕΛΑΚΤ

- **Ομάδα Ασφάλειας Πληροφοριακών Συστημάτων και Δικτύων (ΟΑΠΣΥΔ):** Συγκροτείται από στελέχη της ΔΗΔΕΠ και της ΜΕΕ κατόπιν έκδοσης σχετικής Απόφασης κ. Υ.ΝΑ.Ν.Π..

- **Υπεύθυνος Πληροφοριακού Συστήματος (ΥΠΣ):** Είναι το στέλεχος ή ομάδα στελεχών που ορίζονται με Ημερήσια Διαταγή ή Απόφαση Προϊσταμένου από κάθε Κεντρική Υπηρεσία-Διεύθυνση του Φορέα, η οποία είναι αρμόδια για την αξιοποίηση, χρήση και επιχειρησιακή λειτουργία πληροφοριακού συστήματος - εφαρμογής, εφόσον υφίστανται.

2.4. Τοπικοί διαχειριστές ΠΣ

Ο Τοπικός Διαχειριστής ΠΣ (ΤΔΠΣ), εφόσον αυτό υφίσταται, είναι το στέλεχος που ορίζεται με Ημερήσια Διαταγή ή Απόφαση Προϊσταμένου από κάθε Κεντρική Υπηρεσία-Διεύθυνση του Φορέα και είναι υπεύθυνος για την ορθή λειτουργία **εκάστου** ΠΣ, για το οποίο διαθέτει αυξημένα δικαιώματα πρόσβασης. Για κάθε ΠΣ θα ορίζεται ένας ΤΔΠΣ.

2.5. Χρήστες

Οι τελικοί χρήστες των ΠΣ.

2.6. Αρμοδιότητες - υποχρεώσεις δομών ΛΣ-ΕΛ.ΑΚΤ.

2.6.1. Αρμοδιότητες ΔΗΔΕΠ

Οι αρμοδιότητες της ΔΗΔΕΠ είναι οι ακόλουθες:

- Η ανάπτυξη και η εφαρμογή της πολιτικής ασφαλείας βάσει του Π.Δ. 13/2018.

- Διαρκής ενημέρωση και ευαισθητοποίηση όλων των χρηστών Λ.Σ-ΕΛ.ΑΚΤ. περί των βασικών μέτρων ασφάλειας ως περιγράφονται στην παρούσα ΠΑ και της ορθής εφαρμογής τους.

- Παρακολούθηση και διερεύνηση περιστατικών παραβίασης πολιτικής ασφαλείας σε συνεργασία με τον ΥΠΣ και τους ΤΔΠΣ.

- Ενημέρωση ΟΑΠΣΥΔ σχετικά με το αποτέλεσμα της διερεύνησης των περιστατικών παραβίασης πολιτικής ασφαλείας.

- Λήψη αποφάσεων σχετικά με τα πρότυπα και τις μεθόδους που πρέπει να χρησιμοποιούνται για την ανάπτυξη, εγκατάσταση και ασφαλή λειτουργία ενός ΠΣ ή δικτύου.

- Κίνηση διαδικασίας υποβολής προτάσεων για τον ανασχεδιασμό - επικαιροποίηση της ΠΑ σε συνεργασία με την ΟΑΠΣΥΔ, σε τακτική βάση ή όποτε απαιτηθεί.

2.6.2. Αρμοδιότητες ΜΕΕ-ΛΣ.ΑΚΤ.

Αφορούν στον έλεγχο πληροφοριακών συστημάτων, προκειμένου να διαπιστωθεί κατά πόσον επιτυγχάνουν τους σκοπούς τους και εάν έχουν ενσωματωθεί σε αυτά επαρκείς ασφαλιστικές δικλείδες/μηχανισμοί ελέγχου.

2.6.3. Αρμοδιότητες ΟΑΠΣΥΔ

Οι αρμοδιότητες της ΟΑΠΣΥΔ είναι οι ακόλουθες:

- Έλεγχος εφαρμογής της ΠΑ

- Παρακολούθηση των περιστατικών που σχετίζονται με την ασφάλεια των ΠΣ του Λ.Σ-ΕΛ.ΑΚΤ. και εισηγείται στη ΔΗΔΕΠ περί της αναγκαιότητας ή μη, τροποποίησης της ΠΑ.

2.6.4. Αρμοδιότητες ΥΠΣ

Οι αρμοδιότητες του ΥΠΣ είναι οι ακόλουθες:

- Εφαρμογή της ΠΑ σε συνεργασία με τους τοπικούς διαχειριστές ΠΣ

- Υλοποίηση μέτρων που αφορούν στην αντιμετώπιση περιστατικών παραβίασης της πολιτικής ασφάλειας μόλις αυτά γίνουν αντιληπτά σε συνεργασία με τους τοπικούς διαχειριστές ΠΣ.

- Ενημέρωση της ΟΑΠΣΥΔ και της ΔΗΔΕΠ σε περιπτώσεις παραβίασης ασφάλειας.

- Διαρκής ενημέρωση και ευαισθητοποίηση όλων των χρηστών των ΠΣ αρμοδιότητάς του περί των βασικών μέτρων ασφάλειας και της ορθής εφαρμογής τους.

2.6.5. Αρμοδιότητες τοπικού διαχειριστή

Οι αρμοδιότητες του ΤΔΠΣ είναι οι ακόλουθες:

- Εφαρμογή της ΠΑ στα ΠΣ αρμοδιότητάς τους

- Υλοποίηση μέτρων που αφορούν την αντιμετώπιση περιστατικών παραβίασης της πολιτικής ασφαλείας μόλις αυτά γίνουν αντιληπτά.

- Ενημέρωση του ΥΠΣ σε περιπτώσεις παραβίασης ασφάλειας.

- Υποβοηθά το έργο των αρμοδίων σε περιπτώσεις διερεύνησης περιστατικών παραβίασης ΠΑ.

- Τήρηση αρχείου των δικαιωμάτων πρόσβασης των εξουσιοδοτημένων χρηστών στα ΠΣ αρμοδιότητάς του.

- Ο τοπικός διαχειριστής των ΠΣ διαμορφώνει τα ΠΣ έτσι ώστε οι χρήστες να έχουν πρόσβαση και να μπορούν να εκτελούν μόνο εργασίες για τις οποίες έχουν εξουσιοδοτηθεί.

2.6.6. Υποχρεώσεις χρηστών

Οι χρήστες των ΠΣ του ΛΣ-ΕΛ.ΑΚΤ οφείλουν να γνωρίζουν τις υποχρεώσεις που προκύπτουν από την ΠΑ.

Συγκεκριμένα οι χρήστες δεσμεύονται ότι:

- Οι πληροφορίες του ΛΣ-ΕΛ.ΑΚΤ που είναι αποθηκευμένες σε ηλεκτρονικό και μηχανογραφικό εξοπλισμό παραμένουν στην κυριότητα του ΛΣ-ΕΛ.ΑΚΤ.

- Οι χρήστες είναι υποχρεωμένοι να δηλώνουν άμεσα κλοπή, απώλεια, ή μη εξουσιοδοτημένη τροποποίηση ή αποκάλυψη πληροφοριών του ΛΣ-ΕΛ.ΑΚΤ.

- Η πρόσβαση στις πληροφορίες του ΛΣ-ΕΛ.ΑΚΤ γίνεται μόνο στον βαθμό που υπάρχει εξουσιοδότηση και με βάση τις αρμοδιότητες που έχουν ανατεθεί.

- Οι αρμόδιες δομές του ΛΣ-ΕΛ.ΑΚΤ διατηρούν το δικαίωμα να ελέγχουν περιοδικά την συμμόρφωση των χρηστών των ΠΣ με την ΠΑ.

- Απαγορεύεται η αποκάλυψη του κωδικού ασφαλείας σε τρίτους, η αναγραφή των κωδικών σε εμφανή σημεία καθώς και η χρήση του λογαριασμού ενός χρήστη ΠΣ από άλλον χρήστη.

2.6.7. Στελέχωση ομάδων

Για την ορθή, απρόσκοπτη και αντικειμενική λειτουργία των δομών που περιγράφονται παραπάνω ισχύουν τα ακόλουθα:

- Στον τοπικό διαχειριστή δύναται να αποδοθεί ο ρόλος του ΥΠΣ.

- Ο τοπικός διαχειριστής και ο ΥΠΣ δεν μπορούν να συμμετέχουν ως μέλη στην ΟΑΠΣΥΔ.

ΜΕΡΟΣ Β

3. Πληροφοριακά συστήματα

Πληροφοριακά συστήματα ονομάζεται ένα σύνολο διαδικασιών, ανθρώπινου δυναμικού και αυτοματοποιημένων υπολογιστικών συστημάτων, που προορίζονται για τη συλλογή, εγγραφή, ανάκτηση, επεξεργασία, αποθήκευση και ανάλυση δεδομένων-πληροφοριών. Τα συστήματα αυτά μπορούν να περιλαμβάνουν λογισμικό, υλικό και τηλεπικοινωνιακό σκέλος.

Σκοπός του κεφαλαίου είναι να διαμορφώσει ένα σύνολο κανόνων και διαδικασιών το οποίο θα ενεργήσει προληπτικά με στόχο να περιορίσει στο ελάχιστο την πιθανότητα μη εξουσιοδοτημένης πρόσβασης στα πληροφορικά συστήματα του Φορέα.

3.1. Σχεδιασμός πληροφοριακών συστημάτων

Πληροφοριακά Συστήματα που προσφέρουν υπηρεσίες και είναι προσπελάσιμα από πολλούς χρήστες πρέπει να ικανοποιούν κατ' ελάχιστον τα παρακάτω:

- Να παρέχουν αναγνώριση της ταυτότητας του χρήστη που έχει πρόσβαση στο σύστημα.
- Όπου είναι εφικτό, να υπάρχει περιορισμός του χρόνου σύνδεσης του χρήστη στο σύστημα ή την εφαρμογή.
- Η πρόσβαση στα πληροφοριακά συστήματα θα είναι επιτρεπτή μόνο αφού έχει προηγηθεί διαδικασία πιστοποίησης ταυτότητας μεταξύ του χρήστη και κάθε συστήματος.
- Δεν επιτρέπεται η πρόσβαση σε πληροφοριακά συστήματα με μη ατομικούς λογαριασμούς χρηστών.
- Η πρόσβαση στα επιμέρους πληροφοριακά συστήματα γίνεται μόνο μέσω του κεντρικού συστήματος αυθεντικοποίησης που διαθέτει ο Φορέας.

3.2. Διαδικασία σύνδεσης (login) των χρηστών

Η διαδικασία σύνδεσης (login) διασφαλίζει ότι μη εξουσιοδοτημένοι χρήστες δεν θα αποκτήσουν πρόσβαση στο σύστημα. Αυτό σημαίνει ότι δεν πρέπει να αποκαλύπτονται πληροφορίες για το σύστημα οι οποίες ενδέχεται να βοηθήσουν τον μη εξουσιοδοτημένο χρήστη να αποκτήσει πρόσβαση. Μερικές ενέργειες που συντελούν σ' αυτό είναι:

- Μη εμφάνιση των κωδικών αναγνώρισης του συστήματος μέχρι να ολοκληρωθεί η διαδικασία σύνδεσης.
- Εμφάνιση μηνύματος ότι μόνο εξουσιοδοτημένοι χρήστες επιτρέπεται-δύναται να έχουν πρόσβαση στο σύστημα.
- Μη παροχή βοήθειας κατά τη διαδικασία εισόδου (login).
- Πιστοποίηση των πληροφοριών σύνδεσης, μόνον μετά την εισαγωγή όλων των δεδομένων εισόδου. Σε περίπτωση αποτυχίας σύνδεσης το σύστημα δεν επισημαίνει σε ποιο τμήμα ήταν το λάθος.
- Περιορισμός των επιτρεπόμενων προσπαθειών σύνδεσης σε τρεις. Καταγράφονται από το σύστημα οι ανεπιτυχείς προσπάθειες. Μετά τις τρεις προσπάθειες επιβάλλεται χρονική καθυστέρηση μέχρι να επιτραπεί στο χρήστη η επανάληψη της προσπάθειας σύνδεσης.

- Μετά την ολοκλήρωση της διαδικασίας, εμφανίζεται η τελευταία ημερομηνία και ώρα επιτυχούς login, καθώς και λεπτομέρειες για όποιες ανεπιτυχείς απόπειρες login μεσολάβησαν.

3.3. Παρακολούθηση πρόσβασης και χρήσης

Οι προσβάσεις των χρηστών στα ΠΣ καθώς και οι ενέργειές τους παρακολουθούνται και καταγράφονται έτσι ώστε να αποφεύγονται μη εξουσιοδοτημένες ενέργειες, να εξασφαλίζεται η εναρμόνιση των χρηστών και των συστημάτων με την ΠΑ και να διευκολύνεται το έργο της διερεύνησης σε περιστατικά παραβίασης ΠΑ. Τα ΠΣ θα πρέπει κατ' ελάχιστον να διαθέτουν την δυνατότητα για:

- Εργαλεία για την καταγραφή συμβάντων (Event Logging).
- Εργαλεία για την παρακολούθηση χρήσης συστημάτων (System Monitoring).

3.4. Δημιουργία/ Διαγραφή χρηστών

Η δημιουργία καθώς και η διαγραφή λογαριασμών χρηστών στο κεντρικό σύστημα αυθεντικοποίησης του Φορέα πραγματοποιείται σύμφωνα με συγκεκριμένη διαδικασία η οποία καθορίζεται από το αρμόδιο Τμήμα της ΔΗΔΕΠ. Με τη δημιουργία του λογαριασμού, οι χρήστες αποδέχονται τα αναφερόμενα στην παρούσα ΠΑ.

3.5. Usernames – passwords(credentials)

Η μέθοδος που χρησιμοποιείται για την πιστοποίηση των εξουσιοδοτημένων χρηστών από τα συστήματα είναι η χρήση των κωδικών πρόσβασης, δηλαδή ο μοναδικός κωδικός αναγνώρισης ταυτότητας χρήστη/όνομα χρήστη (username) σε συνδυασμό με τον κωδικό ασφάλειας (password).

Κωδικός αναγνώρισης ταυτότητας χρήστη/Όνομα χρήστη (username)

Όλοι οι χρήστες έχουν έναν μοναδικό, ατομικό κωδικό αναγνώρισης ταυτότητας χρήστη/όνομα χρήστη (username). Οι κωδικοί αναγνώρισης δεν δίνουν ενδείξεις για τα προνόμια που κατέχει ο κάθε χρήστης, δημιουργούνται δε με προκαθορισμένο τρόπο ο οποίος καθορίζεται από τη ΔΗΔΕΠ.

Κωδικός ασφάλειας χρηστών (password)

Οι κωδικοί πρέπει να δίδονται στους χρήστες με ασφαλή τρόπο. Οι νέοι κωδικοί που θα εισάγουν οι χρήστες πρέπει να επιλέγονται βάσει των όσων περιγράφονται στη συνέχεια και σύμφωνα με εξειδικευμένους κανόνες που τίθενται από τη ΔΗΔΕΠ.

Η κύρια αδυναμία οποιουδήποτε συστήματος κωδικών ασφάλειας είναι η επιλογή από τους χρήστες κωδικών οι οποίοι είναι εύκολο να μαντέψει ένας επίδοξος εισβολέας. Ένας τρόπος για την εξάλειψη αυτής της πιθανότητας είναι η μη χρήση συνηθισμένων κωδικών ασφαλείας. Ενδεικτικά αναφέρεται η αποφυγή κωδικών που βασίζονται σε μήνες του χρόνου, ημέρες της εβδομάδας ή οποιαδήποτε άλλη μορφή ημερομηνίας, ονόματα, αρχικά ή αριθμούς κυκλοφορίας αυτοκινήτων, ταυτότητα, αριθμούς τηλεφώνων κ.λπ.. Επίσης προτείνεται η χρήση ολόκληρων φράσεων με μήκος παραπάνω από 15 χαρακτήρες και όχι μεμονωμένων λέξεων.

Οι κωδικοί πρόσβασης είναι αυστηρά προσωπικοί και πρέπει να τηρούνται εμπιστευτικοί. Σε καμία περίπτωση δεν πρέπει ο χρήστης να πληροφορεί τρίτους για τον ατομικό του κωδικό ασφάλειας και να τους επιτρέπει να τον χρησιμοποιήσουν για πρόσβαση ΠΣ ή σταθμό εργασίας. Γενικά να αποφεύγεται η τήρηση εγγράφων που περιέχουν τους κωδικούς ασφάλειας ενώ δεν πρέπει να

σημειώνονται σε χαρτί ή άλλο μέσο, το οποίο μπορεί να διαβάσει ο οποιοσδήποτε, ειδικότερα στην περιοχή που βρίσκεται το τερματικό. Είναι πολύ σημαντικό να απομνημονεύει ο κάθε χρήστης τον κωδικό του.

Δεν πρέπει να συμπεριλαμβάνουν την είσοδο του κωδικού ασφάλειας σε αυτοματοποιημένες διαδικασίες login (π.χ. αποθήκευση κωδικών σε browser).

3.6. Χρήση πληροφοριακών συστημάτων

Η ορθή και ασφαλή χρήση ΠΣ προϋποθέτει τα ακόλουθα σημεία:

- Κάθε χρήστης αποκτά πρόσβαση μόνο σε πληροφοριακά συστήματα για τα οποία του έχει εκχωρηθεί σχετική εξουσιοδότηση από τον ΤΔΠΣ.
- Η πρόσβαση στα πληροφοριακά συστήματα θα είναι επιτρεπτή μόνο αφού έχει προηγηθεί διαδικασία πιστοποίησης ταυτότητας μεταξύ του χρήστη και του συγκεκριμένου συστήματος.
- Επιβάλλεται η χρήση ατομικών κωδικών πρόσβασης για κάθε χρήστη και απαγορεύεται η χρήση κωδικών πρόσβασης άλλων χρηστών.
- Δεν επιτρέπεται η πρόσβαση σε πληροφοριακά συστήματα με μη ατομικούς λογαριασμούς χρηστών.
- Η πρόσβαση στα επιμέρους πληροφοριακά συστήματα θα γίνεται μέσω του κεντρικού συστήματος αυθεντικοποίησης που διαθέτει ο Φορέας.
- Οι ενέργειες των χρηστών, καταγράφονται από εργαλεία παρακολούθησης των συστημάτων και των εφαρμογών. Τα σχετικά αρχεία καταγραφής των ενεργειών τους (πχ eventlog) δύνανται να αναζητηθούν μέσω των τοπικών διαχειριστών των συστημάτων.
- Τα δικαιώματα πρόσβασης των χρηστών δύνανται να τροποποιηθούν.

4. Πρόσβαση στα ΠΣ

4.1. Πρόσβαση χρηστών Φορέα από το εσωτερικό δίκτυο

Αφορά στην πρόσβαση των στελεχών του Φορέα στα ΠΣ αρμοδιότητάς τους από το τοπικό δίκτυο και περιορίζεται στα ΠΣ για τα οποία έχουν εξουσιοδοτηθεί.

4.2. Απομακρυσμένη πρόσβαση χρηστών Φορέα

Αφορά στην πρόσβαση των στελεχών του Φορέα στα ΠΣ αρμοδιότητάς τους από απομακρυσμένα σημεία. Αυτή, εφόσον κρίνεται αναγκαία από τη ΔΗΔΕΠ, θα πραγματοποιείται από τους χρήστες με την ίδια σοβαρότητα και βαρύτητα όπως και σε αντίστοιχη σύνδεση από σταθμό εργασίας εντός του δικτύου του Φορέα. Επιπλέον μέτρα που πρέπει να λαμβάνονται αφορούν:

- Τη διατήρηση της φυσικής ασφάλειας και την λήψη απαραίτητων μέτρων για την αποφυγή κλοπής ή απώλειας των συσκευών, λογισμικών ή δεδομένων διαπίστευσης που χρησιμοποιούνται για την απομακρυσμένη πρόσβαση.

- Την ασφαλή πρόσβαση στις συσκευές με χρήση κωδικού καθώς και την ασφαλή πρόσβαση στα ΠΣ του ΛΣ-ΕΛ.ΑΚΤ με χρήση κωδικών και κρυπτογράφησης.

- Την εγκατάσταση λογισμικού μόνο από έμπιστες πηγές στις συσκευές που χρησιμοποιούνται για την απομακρυσμένη πρόσβαση και την συνεχή ενημέρωσή του.

- Τη μη ανάγνωση εμπιστευτικών πληροφοριών σε δημόσιο χώρο.

- Η απομακρυσμένη πρόσβαση θα ενεργοποιείται εφόσον υπάρχει υπηρεσιακή ανάγκη κατόπιν σχετικής αλληλογραφίας και θα τερματίζει με την ολοκλήρωση αυτής.

4.3. Πρόσβαση εξωτερικών χρηστών

Αφορά στην πρόσβαση εξωτερικών χρηστών στα ΠΣ του Φορέα και διακρίνεται στα ακόλουθα δύο είδη:

4.3.1. Τοπική πρόσβαση

Αφορά στην πρόσβαση εξωτερικών χρηστών στα ΠΣ του Φορέα από το εσωτερικό δίκτυο με επιτόπια παρουσία αυτών στις εγκαταστάσεις. Η χρήση προσωπικών υπολογιστών εξωτερικών χρηστών εντός του εσωτερικού δικτύου επιτρέπεται αποκλειστικά και μόνο για τα δίκτυα διαχείρισης των συστημάτων και θα πραγματοποιείται υπό την επίβλεψη των τοπικών διαχειριστών.

4.3.2. Απομακρυσμένη πρόσβαση

Αφορά στην πρόσβαση εξωτερικών χρηστών στα ΠΣ του Φορέα από το εξωτερικό δίκτυο (δίκτυο ΣΥΖΕΥΞΙΣ, Ίντερνετ, μισθωμένα κυκλώματα κ.λπ.). Δεν επιτρέπεται η απομακρυσμένη πρόσβαση στα ΠΣ του Φορέα με σκοπό την παραμετροποίηση-εγκατάσταση, επιδιόρθωση των ΠΣ.

4.4. Επικοινωνία-Διασύνδεση ΠΣ με τρίτα συστήματα

Η επικοινωνία των ΠΣ του Φορέα με συστήματα τρίτων θα πραγματοποιείται με τρόπο που θα εξασφαλίζει την ασφάλεια και την κρυπτογράφηση των δεδομένων λαμβάνοντας υπόψη την παρούσα ΠΑ. Για κάθε τέτοιου τύπου επικοινωνία θα καταγράφεται με μέριμνα του τοπικού διαχειριστή αναλυτική περιγραφή του τρόπου επικοινωνίας των ΠΣ.

5. Σταθμοί εργασίας

Οι περισσότεροι χρήστες ΠΣ πραγματοποιούν συγκεκριμένες εργασίες οι οποίες προκύπτουν από τα καθήκοντα που τους ανατίθενται και συνεπώς δεν είναι απαραίτητο να τους παραχωρούνται δικαιώματα για όλα τα ΠΣ. Ως εκ τούτου, είναι σκόπιμο να πραγματοποιούνται ρυθμίσεις ώστε για τους περισσότερους χρήστες να εγκαθίσταται ένα τυποποιημένο, περιορισμένο περιβάλλον. Ο όρος τυποποιημένο αναφέρεται στον συνδυασμό τυποποιημένου υλικού, λογισμικού και διαμόρφωσης – παραμετροποίησης αυτών. Ο σχεδιασμός και η εγκατάσταση τυποποιημένων σταθμών εργασίας υλοποιείται από εξειδικευμένο προσωπικό λαμβάνοντας υπόψη την εργασία, την αξιοπιστία, την εργονομία, την ταχύτητα και τη δυνατότητα χρήσης. Σκοπός είναι, αφενός η παρεμπόδιση χρήσης λειτουργιών που δεν απαιτούνται από τα καθήκοντα του χρήστη, αφετέρου η αποφυγή προβλημάτων λόγω άγνοιας, καθώς υπάρχει περίπτωση εκτέλεσης κάποιας λειτουργίας από λάθος, η οποία μπορεί να επιφέρει αλλοίωση στα δεδομένα ή βλάβη.

Κατά τη χρήση των σταθμών εργασίας θα πρέπει κάθε χρήστης να εφαρμόζει τους ακόλουθους κανόνες.

- Όλες οι συσκευές ηλεκτρονικών υπολογιστών ιδιοκτησίας του ΛΣ-ΕΛ.ΑΚΤ πρέπει να προστατεύονται από κωδικό ασφαλείας.

- Οι χρήστες οφείλουν να απενεργοποιούν τους σταθμούς εργασίας και τον περιφερειακό εξοπλισμό μετά το πέρας εργασίας.

- Οι χρήστες οφείλουν να κλειδώνουν (LockScreen, κλείδωμα οθόνης) το τερματικό τους όταν απομακρύνονται από αυτό και να έχουν ενεργοποιημένη την Προστασία Οθόνης (screensaver) με χρήση συνθηματικού για την επαναφορά.

- Οι χρήστες οφείλουν να χρησιμοποιούν μόνο εξουσιοδοτημένο υλικό και λογισμικό.

- Οι χρήστες οφείλουν να λαμβάνουν τακτικά εφεδρικά αντίγραφα των αρχείων τους.

- Δεν επιτρέπεται στους χρήστες η εγκατάσταση ή χρήση λογισμικού πλην των απαραίτητων για την κάλυψη των υπηρεσιακών αναγκών.

- Όλοι οι σταθμοί εργασίας των στελεχών του Φορέα που συνδέονται στο εσωτερικό δίκτυο του Φορέα, διαθέτουν λογισμικό ανίχνευσης και αντιμετώπισης κακόβουλου κώδικα το οποίο οι χρήστες οφείλουν να μην το παρακάμπτουν και να μην το απενεργοποιούν για οποιοδήποτε λόγο. Οι χρήστες επίσης οφείλουν να μην προβαίνουν σε οποιαδήποτε τροποποίησης των ρυθμίσεων του εν λόγω λογισμικού με τρόπο ώστε να μειώνεται η αποτελεσματικότητά του.

- Οι χρήστες οφείλουν σε περίπτωση μη αυτόματης απομάκρυνσης ιού ή κακόβουλου λογισμικού, ή σε περίπτωση σχετικής υποψίας, να ενημερώνουν άμεσα τη ΔΗΔΕΠ και οι Λιμενικές Αρχές το Γραφείο Γραμματείας και Πληροφορικής σύμφωνα με τον Κανονισμό Λειτουργίας των Λιμενικών Αρχών, όπως ισχύει.

- Οι χρήστες οφείλουν να χρησιμοποιούν εξωτερικές συσκευές αποθήκευσης μόνο εφόσον αυτές ελεγχθούν από το λογισμικό ανίχνευσης και αντιμετώπισης κακόβουλου κώδικα.

Στοιχεία που έρχονται σε αντίθεση με την παρούσα ΠΑ είναι τα ακόλουθα:

- Η εγκατάσταση παράνομου ή μη εξουσιοδοτημένου λογισμικού.

- Η παραμετροποίηση των ρυθμίσεων του δικτύου από μη εξουσιοδοτημένο προσωπικό του Φορέα.

- Η απενεργοποίηση ή απεγκατάσταση λογισμικού που έχει εγκατασταθεί από το εξουσιοδοτημένο προσωπικό του Φορέα.

- Η εγκατάσταση μη εξουσιοδοτημένου υλικού εξοπλισμού όπως modem, wireless access points, repeaters, switches κ.λπ. που δύναται όχι μόνο να προκαλέσει δυσλειτουργία στο δίκτυο του Φορέα αλλά ταυτόχρονα και να μειώσει το επίπεδο ασφάλειας.

6. Προστασία του χώρου εργασίας

Τα στελέχη του Φορέα είναι υπεύθυνα για τον χώρο στον οποίο εργάζονται. Οι φορητοί υπολογιστές, τα φορητά εξωτερικά μέσα αποθήκευσης (USB sticks, οπτικοί δίσκοι, εξωτερικοί σκληροί δίσκοι, ΑΔΔΥ) πρέπει να κλειδώνονται σε ασφαλή σημεία (ντουλάπια, συρτάρια, φοριαμούς κ.λπ.). Οι κωδικοί πρόσβασης δεν πρέπει να είναι γραμμένοι σε εμφανές σημείο ή να είναι εύκολα προσβάσιμοι. Τέλος, οι εκτυπώσεις από εκτυπωτικές μηχανές (εκτυπωτές, συσκευές fax) θα πρέπει να απομακρύνονται άμεσα ώστε να αποφεύγεται το ενδεχόμενο απόκτησης της πληροφορίας από μη εξουσιοδοτημένα πρόσωπα.

7. Ηλεκτρονική αλληλογραφία

Μέσω του συστήματος ηλεκτρονικής αλληλογραφίας που διαθέτει ο Φορέας, το προσωπικό του Φορέα έχει τη δυνατότητα να λάβει και να στείλει μηνύματα από και προς ολόκληρο το διαδίκτυο γεγονός που απαιτεί ιδιαίτερη προσοχή καθώς εγκυμονεί πολλούς κινδύνους.

Κατά τη χρήση του συστήματος ηλεκτρονικής αλληλογραφίας θα πρέπει κάθε χρήστης να υιοθετεί τα ακόλουθα:

- Η αποστολή εμπιστευτικών ηλεκτρονικών μηνυμάτων επιτρέπεται μόνο με χρήση μηχανισμών κρυπτογράφησης.
- Τα ηλεκτρονικά μηνύματα που αφορούν ζητήματα ενημέρωσης για νέους ιούς, αποστέλλονται αποκλειστικά και μόνο από το αρμόδιο τμήμα της ΔΗΔΕΠ.
- Η σύνδεση στην υπηρεσία webmail δεν είναι ασφαλές να πραγματοποιείται από κοινόχρηστα μέσα (π.χ. υπολογιστές internet café, internet kiosks κ.λπ.).

Στοιχεία που έρχονται σε αντίθεση με την παρούσα ΠΑ είναι τα ακόλουθα:

- Η χρήση, δημιουργία και η διανομή οποιονδήποτε προσβλητικών μηνυμάτων, συμπεριλαμβανομένων και προσβλητικών μηνυμάτων σχετικά με τη φυλή, το φύλο, τις ανικανότητες, την ηλικία, τους σεξουαλικούς προσανατολισμούς, την πορνογραφία, τα θρησκευτικά πιστεύω, τις πολιτικές απόψεις ή την εθνική προέλευση. Επίσης δεν επιτρέπεται το σύστημα να χρησιμοποιείται για να προσβάλει, να απειλεί, να δυσφημεί και γενικότερα να παρενοχλεί τρίτους.
- Η ανάγνωση εισερχομένων ηλεκτρονικών μηνυμάτων με επισυναπτόμενα αρχεία από άγνωστο αποστολέα ή γνωστό αποστολέα από την τον οποίο ωστόσο δεν αναμένονταν αλληλογραφία, καθώς μπορεί να περιέχουν κακόβουλο λογισμικό.
- Η αποστολή ή προώθηση αλυσιδωτών μηνυμάτων.
- Η αποστολή μηνυμάτων που περιέχουν ιούς ή οποιασδήποτε μορφής αρχεία που μπορούν να δημιουργήσουν προβλήματα σε λογισμικό ή υπολογιστές.
- Η μαζική αποστολή ηλεκτρονικών μηνυμάτων καθώς μπορεί να προκαλέσει δυσλειτουργίες σε υπηρεσίες και δικτυακές συσκευές.
- Η με οποιονδήποτε τρόπο παραποίηση των αναγνωριστικών στοιχείων των ηλεκτρονικών μηνυμάτων που προσδιορίζουν τον αποστολέα.

- Η χρήση του συστήματος ηλεκτρονικής αλληλογραφίας ως σύστημα απόθεσης και διατήρησης αρχείων.

- Η αποθήκευση του λογαριασμού και του κωδικού πρόσβασης στον browser.

Τονίζεται ότι σε καμία περίπτωση δεν θα ζητηθεί από τη ΔΗΔΕΠ η αποστολή προσωπικών στοιχείων του υπηρεσιακού λογαριασμού ηλεκτρονικού ταχυδρομείου (π.χ. όνομα χρήστη, κωδικός πρόσβασης) και ως εκ τούτου τέτοια μηνύματα πρέπει να εκλαμβάνονται ως κακόβουλα και επικίνδυνα, με μόνο στόχο την υπεξαίρεση προσωπικών στοιχείων.

8. Πρόσβαση στο Διαδίκτυο

Το διαδίκτυο αποτελεί το αμεσότερο μέσο άντλησης πληροφοριών για κάθε είδος επαγγελματικής δραστηριότητας. Η χρήση του ωστόσο εγκυμονεί κινδύνους και απαιτεί την θέσπιση ενός ευρύτερου πλαισίου για την ασφάλεια τόσο των ίδιων των χρηστών όσο και της εσωτερικής υποδομής του Φορέα.

Κατά την πρόσβαση στο διαδίκτυο θα πρέπει κάθε χρήστης να εφαρμόζει τους ακόλουθους κανόνες:

- Ενδείκνυται και προτρέπεται η επίσκεψη δικτυακών τόπων που συνάδουν με το υπηρεσιακό αντικείμενο – δραστηριότητα των χρηστών.

- Η πρόσβαση στο διαδίκτυο υλοποιείται μέσω από ειδικούς μηχανισμούς κεντρικής πρόσβασης (firewall, proxy, router) που διαθέτει ο Φορέας οι οποίοι πληρούν τις προϋποθέσεις που τίθενται από την ΠΑ.

- Οι χρήστες δύνανται να χρησιμοποιούν μηχανισμούς κρυπτογράφησης, ως προϋπόθεση, για την αποστολή των εμπιστευτικών πληροφοριών μέσω του Διαδικτύου.

- Οι χρήστες οφείλουν να ενημερώνουν άμεσα τον ΥΠΣ και τη ΔΗΔΕΠ, στην περίπτωση που υποπέσει στην αντίληψη οποιοδήποτε γεγονός ή ευπάθεια ασφάλειας.

Στοιχεία που έρχονται σε αντίθεση με την παρούσα ΠΑ είναι τα ακόλουθα:

- Η παραβίαση ή παράκαμψη των μηχανισμών ασφάλειας που έχει θεσπίσει ο Φορέας για την πρόσβαση στο Διαδίκτυο.

- Η χρήση του διαδικτύου για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε άλλο ΠΣ ή υπηρεσία.

- Η εγκατάσταση μη εξουσιοδοτημένου εξοπλισμού και λογισμικού για τη διασύνδεση με το διαδίκτυο.

- Οι ενέργειες που συνιστούν προσπάθεια παραβίασης (επιτυχή ή μη) της ασφάλειας οποιουδήποτε συστήματος (είτε αφορά τον Φορέα είτε τρίτο) μέσα από το διαδίκτυο.

- Η επίσκεψη διαδικτυακών τόπων με περιεχόμενο που δεν συνάδει με το υπηρεσιακό αντικείμενο – δραστηριότητα των χρηστών.

- Η δημιουργία διαδικτυακών λογαριασμών με ίδιο όνομα χρήστη και κωδικό με αυτά που χρησιμοποιούνται εντός του Φορέα.

- Η αποθήκευση των ονομάτων χρήστη και των κωδικών πρόσβασης στο φυλλομετρητή (Browser).

Επισημαίνεται ότι η πρόσβαση σε διαδικτυακούς τόπους από το εσωτερικό δίκτυο του Φορέα εποπτεύεται με αυτοματοποιημένο τρόπο ώστε να αποφευχθεί η εκτέλεση κακόβουλου λογισμικού.

9. Φυσική και περιβαλλοντική ασφάλεια

9.1. Ασφάλεια φυσικών υποδομών

Τόσο οι πληροφορίες όσο και ο εξοπλισμός που χρησιμοποιείται για την αποθήκευση, επεξεργασία ή τη μεταβίβαση πληροφοριών, είναι ευάλωτα σε φυσικές αλλοιώσεις και καταστροφές από περιβαλλοντικούς παράγοντες (φωτιά, πλημμύρα, σεισμός, κ.λπ.) ή τρομοκρατικές και λοιπές κακόβουλες ενέργειες. Δεδομένου ότι είναι αδύνατη η πλήρης απομάκρυνση-εξάλειψη τέτοιων κινδύνων, οι τελευταίοι θα πρέπει, αφού πρώτα εντοπισθούν, να περιοριστούν και να απομονωθούν ώστε τελικώς να αποκατασταθεί η ορθή και σύμφωνα με την ΠΑ λειτουργία των ΠΣ. Γενικά οι εγκαταστάσεις/υποδομές που φιλοξενούν συστήματα, πληροφορίες και δεδομένα πρέπει να είναι φυλασσόμενες και προστατευμένες από φυσικούς ή άλλους τέτοιους κινδύνους.

Ο μηχανογραφικός και δικτυακός εξοπλισμός ειδικής σημασίας (διακομιστές, δρομολογητές κ.λπ.) πρέπει να είναι εγκατεστημένος σε χώρους, αποκλειστικά διατιθέμενους για το σκοπό αυτό και ειδικά διαμορφωμένους προκειμένου να καλύπτονται πλήρως από πλευράς ασφάλειας και επάρκειας στους τομείς ενέργειας, κλιματισμού και πυρασφάλειας. Τέλος, απαγορεύεται η μη εξουσιοδοτημένη απομάκρυνση ή μετακίνηση εξοπλισμού – λογισμικού πληροφορικής εκτός της Υπηρεσίας.

10.Ανίχνευση, αναφορά & διαχείριση περιστατικών παραβίασης ΠΑ

Η ανίχνευση και αντιμετώπιση περιστατικών παραβίασης της πολιτικής ασφαλείας αποτελεί μια από τις σημαντικότερες λειτουργίες και αφορά το σύνολο των χρηστών του Φορέα.

10.1. Ανίχνευση και αναφορά περιστατικών παραβίασης ΠΑ

Οι χρήστες των ΠΣ υποχρεούνται να αναφέρουν στους αρμόδιους (ΥΠΣ και ΔΗΔΕΠ) κάθε αδυναμία που παρατηρείται στα ΠΣ η οποία μπορεί να θέσει σε κίνδυνο την ασφάλειά τους. Γενικότερα, βλάβες και τυχόν απειλές, περιστατικά ή δυσλειτουργίες ασφάλειας, πρέπει να αναφέρονται αμέσως μόλις γίνονται αντιληπτές.

10.2. Διαχείριση συμβάντων περιστατικών παραβίασης ΠΑ

Αμέσως μετά την αναφορά περιστατικού ασφάλειας διεξάγεται αρμοδίως έρευνα για τον καθορισμό του τρόπου με τον οποίο και του σημείου από το οποίο προήλθε η συγκεκριμένη παραβίαση/βλάβη κ.λπ.. Επίσης λαμβάνονται τα κατάλληλα μέτρα για τη διόρθωση ή την ελαχιστοποίηση των επιπτώσεων της συγκεκριμένης παραβίασης/βλάβης κ.λπ..

Οι συνήθεις πρακτικές έχουν ως εξής:

- Η εγκατάσταση και λειτουργία κεντρικού συστήματος ανίχνευσης παρεισφρήσεων αποτελεί μέρος της κεντρικής μηχανογραφικής – δικτυακής υποδομής ασφαλείας του Φορέα.

- Σε περίπτωση που υπάρχουν ενδείξεις περιστατικού παραβίασης ΠΑ, οι αρμόδιοι συνεργάζονται με σκοπό να διερευνηθεί αν οι ενδείξεις αποτελούν πραγματικό συμβάν ή όχι, καθώς και την προέλευσή τους.

- Σε περίπτωση παραβίασης του Γενικού Κανονισμού Προστασίας Δεδομένων, εφαρμόζονται οι διαδικασίες που προβλέπονται σε αυτόν.

11.Διασφάλιση διαθεσιμότητας

Στόχος της παρούσας ενότητας είναι η καταγραφή των προϋποθέσεων για τη διασφάλιση της ακεραιότητας και διαθεσιμότητας των ΠΣ του ΛΣ-ΕΛ.ΑΚΤ, καθώς και των δεδομένων τους.

11.1. Εφεδρικός εξοπλισμός

Για κάθε κεντρικό επιχειρησιακό ΠΣ πρέπει να υπάρχει διαθέσιμο το εφεδρικό του. Ως εφεδρικό σύστημα νοείται:

Α. Πανομοιότυπο σύστημα που βρίσκεται στον ίδιο ή σε διαφορετικό χώρο

Β. Το ΠΣ όπως έχει ληφθεί από σύστημα αντιγράφων ασφαλείας.

Γ. Η εικονική μηχανή που φιλοξενεί το ΠΣ και η οποία βρίσκεται σε εικονικό περιβάλλον αυξημένης διαθεσιμότητας.

Οι τεχνικές λεπτομέρειες αναφορικά με την εφεδρικότητα του εξοπλισμού καταγράφονται από τους τοπικούς διαχειριστές ερχόμενοι σε συνεννόηση με τη ΔΗΔΕΠ.

11.2. Σχεδιασμός αντιμετώπισης απροόπτων για τη διασφάλιση διαθεσιμότητας

Για την εξασφάλιση της ορθής και αδιάλειπτης εκτέλεσης των λειτουργιών των ΠΣ, απαιτείται η σύνταξη και τακτική επικαιροποίηση ενός σχεδίου αντιμετώπισης έκτακτων περιστατικών. Το σχέδιο αυτό περιλαμβάνει μια σειρά από διαδικασίες και μεθόδους οι οποίες πρέπει να ακολουθούνται σε περιπτώσεις όπου απειλείται η ομαλή λειτουργία των ΠΣ. Οι διαδικασίες και οι μέθοδοι που πρέπει να καθιερωθούν στο σχέδιο αφορούν περιπτώσεις οι οποίες καλύπτονται από την σωστή λειτουργία των εφεδρικών συστημάτων και περιπτώσεις οι οποίες είναι αποτέλεσμα σημαντικών προβλημάτων, ικανών να καταστήσουν αδύνατη την λειτουργία τόσο των κύριων όσο και των εφεδρικών συστημάτων.

Το σχέδιο αντιμετώπισης έκτακτων περιστατικών εκπονείται από τους τοπικούς διαχειριστές των ΠΣ σε συνεργασία με τη ΔΗΔΕΠ και θα πρέπει να καλύπτει και να περιγράφει τις διαδικασίες εξασφάλισης της διαθεσιμότητας εκάστου ΠΣ.