

ΑΠΟΦΑΣΗ**Έγκριση της «Πολιτικής Ενημέρωσης και Εκπαίδευσης Προσωπικού σε θέματα ασφάλειας πληροφοριών»**

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ),

Έχοντας υπόψη:

1. Τις διατάξεις:

- α. του Ν. 4070/2012 «*Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις*» (ΦΕΚ 82/Α/2012), όπως ισχύει τροποποιηθείς,
- β. του Ν. 4053/2012 «*Ρύθμιση λειτουργίας της ταχυδρομικής αγοράς, θεμάτων ηλεκτρονικών επικοινωνιών και άλλες διατάξεις*» (ΦΕΚ 44/Α/2012), όπως ισχύει τροποποιηθείς,
- γ. του Ν. 4727/2020 «*Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) – Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις.*» (ΦΕΚ 184/Α/2020),
- δ. του Κανονισμού (ΕΕ) αριθ. 679/2016 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 ή ΓΚΠΔ),
- ε. του Ν. 4624/2019 «*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*» (ΦΕΚ 137/Α/2019),

- στ. του Ν. 4577/2018 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις», (ΦΕΚ 199/ Α' /03-12-2018), όπως ισχύει,
- ζ. του Ν. 4961/2022 «Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις», (ΦΕΚ 146/Α' /27-7-2022),
2. Την ΑΠ 996/08/22-06-2021 Απόφαση της ΕΕΤΤ «Έγκριση Οργανισμού της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων» (ΦΕΚ 3367/Β' /2021),
 3. Την ΑΠ 1004/40/30-8-2021 Απόφαση της ΕΕΤΤ «Κανονισμός Λειτουργίας της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)» (ΦΕΚ 4660/Β' /8-10-2021), όπως ισχύει τροποποιηθείσα με την ΑΠ 1062/18/24-01-2023 (ΦΕΚ 947/Β' /2023),
 4. Την ΑΠ 852/19/21-05-2018 Απόφαση της ΕΕΤΤ «Ορισμός Υπευθύνου Προστασίας Δεδομένων της ΕΕΤΤ σύμφωνα με τον Κανονισμό (ΕΕ) 679/2016 (Γενικός Κανονισμός για την Προστασία Δεδομένων)»,
 5. Την ΑΠ 1017/32/29-11-2021 Απόφαση της ΕΕΤΤ «Ορισμός Υπευθύνου Ασφάλειας των Πληροφοριών (ΥΑΠ - CISO)»,
 6. Την ΑΠ 1021/33/29-12-2021 Απόφαση της ΕΕΤΤ «Ορισμός Υπευθύνου Ασφάλειας Πληροφοριακών Συστημάτων (ΥΑΠΣ), Υπευθύνου Φυσικής Ασφάλειας (ΥΦΑ) και Συγκρότηση Επιτροπών Ασφάλειας που προκύπτουν από τον Κανονισμό της ΕΕΤΤ»,
 7. Την εγκεκριμένη από τον Πρόεδρο της ΕΕΤΤ «Πολιτική Ασφαλείας της ΕΕΤΤ, έκδοση 1.0» με αριθ. πρωτ. 278/1-6-2018,
 8. Την ΑΠ 989/25/26-04-2021 Απόφαση της ΕΕΤΤ «Έγκριση της εφαρμογής της αναθεωρημένης “Πολιτικής Αποδεκτής Χρήσης των Πληροφοριακών Αγαθών της ΕΕΤΤ”»,
 9. Την ΑΠ 1046/15/10-10-2022 Απόφαση της ΕΕΤΤ «Έγκριση της “Πολιτικής Τηλεργασίας και Φορητών Συσκευών”»,

10. Την ΑΠ 1048/13/24-10-2022 Απόφαση της ΕΕΤΤ «Έγκριση της “Πολιτικής Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών”»,
11. Την ΑΠ 1050/26/07-11-2022 Απόφαση της ΕΕΤΤ «Έγκριση της “Πολιτικής Φυσικής και Περιβαλλοντικής Ασφάλειας”»,
12. Την ΑΠ 1069/13/27-03-2023 Απόφαση της ΕΕΤΤ «Έγκριση της “Πολιτικής Ασφάλειας Τελικού Χρήστη”»,
13. Την ΑΠ 1035/9/20-06-2022 Απόφαση της ΕΕΤΤ «Συγκρότηση Ομάδας Εργασίας για την εφαρμογή του Κανονισμού λειτουργίας της ΕΕΤΤ σε σχέση με τα θέματα ασφάλειας πληροφοριών» (ΑΔΑ: ΩΔΜΦ639-ΝΤΜ),
14. Τη με αριθ. πρωτ. 47915/10-05-2023 Απόφαση του Προέδρου της ΕΕΤΤ «Αποζημίωση μελών Ομάδας Εργασίας με αντικείμενο την εφαρμογή του Κανονισμού λειτουργίας της ΕΕΤΤ σε σχέση με τα θέματα ασφάλειας πληροφοριών» (ΑΔΑ: 9ΙΠΚ639-ΒΥΡ),
15. Την Εισήγηση αριθ. 36897/15-06-2023 της αρμόδιας Υπηρεσίας της ΕΕΤΤ, και ύστερα από προφορική εισήγηση του Προέδρου της ΕΕΤΤ (Καθηγητή Κωνσταντίνου Μασσέλου),

Επειδή :

Α. Το προσωπικό της ΕΕΤΤ και οι εξωτερικοί συνεργάτες που χρησιμοποιούν τα πληροφοριακά συστήματα και την πληροφορία της οφείλουν να είναι όσο το δυνατόν περισσότερο ευαισθητοποιημένοι στην ασφάλεια των πληροφοριών και υποδομών της και ενημερωμένοι στις πολιτικές ασφαλείας της. Με τον τρόπο αυτό, θα διασφαλίζεται η ετοιμότητά τους στην αναγνώριση απειλών και συμβάντων κυβερνοασφάλειας, η συνεισφορά τους στην αποτελεσματική αντιμετώπιση και ο περιορισμός του βαθμού έκθεσης της ΕΕΤΤ σε κινδύνους που δύναται να προέλθουν «εκ των έσω» από ενέργειες του προσωπικού.

Β. Έως τώρα η ΕΕΤΤ έχει παράσχει, αποσπασματικά, πληροφόρηση στο προσωπικό της για την προστασία προσωπικών δεδομένων και την ασφάλεια. Κρίνεται σκόπιμη η έγκριση και λειτουργία μιας πολιτικής ενημέρωσης και εκπαίδευσης του προσωπικού στα

θέματα ασφάλειας πληροφοριών, η οποία θα θέτει τους κανόνες που θα ακολουθούνται εφεξής.

Γ. Με την υπό στοιχείο 13. ως άνω απόφαση της ΕΕΤΤ συγκροτήθηκε ομάδα εργασίας με αντικείμενο την εφαρμογή του Κανονισμού λειτουργίας της ΕΕΤΤ σε σχέση με τα θέματα ασφάλειας πληροφοριών. Ειδικότερα, στα αντικείμενα της ομάδας ήταν, μεταξύ άλλων, ο προσδιορισμός των αναγκών εκπαίδευσης σε θέματα ασφάλειας τόσο των αρμόδιων Επιτροπών/Ομάδων που ορίζονται στον υπό στοιχείο 3 ως άνω Κανονισμό Λειτουργίας όσο και του συνόλου των στελεχών της ΕΕΤΤ, καθώς και η πρόταση και ο προγραμματισμός σχετικών προγραμμάτων εκπαίδευσης.

Δ. Με την υπό στοιχείο 14. ως άνω απόφαση του Προέδρου της ΕΕΤΤ βεβαιώθηκε το καλώς έχειν του έργου της ανωτέρω ομάδας εργασίας για το χρονικό διάστημα από την 01/02/2023 έως τις 30/4/2023. Στο έργο αυτό συμπεριλαμβάνονταν, μεταξύ άλλων, το παραδοτέο της ομάδας με τις προτάσεις της για τις «Εκπαιδευτικές Δράσεις για την Κυβερνοασφάλεια». Παράρτημα του παραδοτέου αυτού αποτελούσε η «Πολιτική Ενημέρωσης και Εκπαίδευσης Προσωπικού σε θέματα ασφάλειας πληροφοριών», που παρουσιάζεται παρακάτω.

Αποφασίζει :

Α. **Εγκρίνει** την «Πολιτική Ενημέρωσης και Εκπαίδευσης Προσωπικού σε θέματα ασφάλειας πληροφοριών», η οποία στοχεύει στην καλλιέργεια κουλτούρας ασφάλειας στην ΕΕΤΤ και καθορίζει τις κύριες αρχές σύμφωνα με τις οποίες θα γίνεται η ευαισθητοποίηση και εκπαίδευση του προσωπικού καθώς και των εξωτερικών συνεργατών της ΕΕΤΤ που χρησιμοποιούν τα πληροφοριακά συστήματα και την πληροφορία της.

Η «Πολιτική Ενημέρωσης και Εκπαίδευσης Προσωπικού σε θέματα ασφάλειας πληροφοριών» έχει ως εξής:

Πολιτική Ενημέρωσης και Εκπαίδευσης Προσωπικού σε θέματα ασφάλειας πληροφοριών

Έκδοση: 1^η

Τελευταία Ημερομηνία Ενημέρωσης: Ιούνιος 2023



1. Σκοπός και Πεδίο Εφαρμογής

Σκοπός της παρούσας πολιτικής είναι να διασφαλίσει ότι η EETT οργανώνει αποτελεσματικές εκπαιδεύσεις και ενθαρρύνει τη συμμετοχή των υπαλλήλων της σε εκστρατείες ενημέρωσης αναφορικά με θέματα ασφάλειας πληροφοριών.

Η συγκεκριμένη πολιτική απευθύνεται σε όλους τους χρήστες των οποίων τα υπηρεσιακά καθήκοντα σχετίζονται με τον κύκλο ζωής των πληροφοριακών συστημάτων της EETT και καλύπτει θέματα σχετικά με:

- Γενικότερη ευαισθητοποίηση και εκπαίδευση των χρηστών.
- Ευαισθητοποίηση των χρηστών σχετικά με την ασφάλεια σε συγκεκριμένους τομείς.

Το πεδίο εφαρμογής της παρούσας πολιτικής περιλαμβάνει τους πληροφοριακούς πόρους της EETT (άνθρωποι, διαδικασίες, τεχνολογία).

2. Ευαισθητοποίηση και Εκπαίδευση Χρηστών

2.1 Αρχές ευαισθητοποίησης σχετικά με την ασφάλεια

Η EETT θα πρέπει να διασφαλίζει ότι τόσο οι εργαζόμενοί της όσο και οι εξωτερικοί συνεργάτες της (όπως φοιτητές που κάνουν πρακτική άσκηση ή ασκούμενοι δικηγόροι κτλ.) συμμορφώνονται με την Πολιτική Ασφάλειας της EETT. Για να επιτευχθεί αυτό, η EETT θα πρέπει να παρέχει εισαγωγική εκπαίδευση και ενημερώσεις σε τακτική βάση στους υπαλλήλους της, καθώς και στους εξωτερικούς της συνεργάτες, προτού επιτρέψει τη φυσική ή λογική τους πρόσβαση στις εγκαταστάσεις, τα συστήματα ή τα δεδομένα της.

2.2 Γενικές αρχές εκπαίδευσης

Η EETT θα πρέπει να διασφαλίζει ότι η εκπαίδευση σχετικά με την ασφάλεια πληροφοριών παρέχεται σε όλους τους χρήστες, έτσι ώστε να λαμβάνουν γνώση της αποδεκτής χρήσης των πληροφοριακών πόρων, τις πειθαρχικές ή άλλου είδους επιπτώσεις στους χρήστες σε περίπτωση μη συμμόρφωσης και τους τρόπους με τους οποίους παρακολουθούνται τα πληροφοριακά συστήματα για να διασφαλίζεται η επιχειρησιακή τους συνέχεια.

2.3 Εκπαιδεύσεις ανάλογα με τους επιχειρησιακούς ρόλους

Η EETT θα πρέπει να υιοθετεί μία σειρά από διαφορετικές τεχνικές για την ενημέρωση και την εκπαίδευση των υπαλλήλων της και των εξωτερικών συνεργατών της στον τομέα της ασφάλειας πληροφοριών, προσαρμοσμένες στους ρόλους και ευθύνες τους, καθώς και τις επιχειρησιακές απαιτήσεις της.

2.4 Συνεχής αξιολόγηση των αναγκών εκπαίδευσης

Οι γνώσεις των χρηστών σε θέματα ασφάλειας πληροφοριών θα πρέπει να αξιολογούνται τακτικά ώστε να εντοπίζονται τυχόν σημεία βελτίωσης. Με βάση την αξιολόγηση αυτή θα κριθεί και αν απαιτείται ενίσχυση του εκπαιδευτικού προγράμματος που παρέχεται.

2.5 Υποχρεωτική συμμετοχή στα εκπαιδευτικά προγράμματα

Οι χρήστες πρέπει να παρακολουθούν τα εκπαιδευτικά προγράμματα και τα σεμινάρια που οργανώνει η EETT σχετικά με το ρόλο και τις ευθύνες που έχουν σε θέματα ασφάλειας πληροφοριών.

Τα εκπαιδευτικά προγράμματα θα πρέπει να οργανώνονται σε επήσια βάση.

2.6 Ενημέρωση των νέων υπαλλήλων σε θέματα ασφάλειας πληροφοριών

Η ενημέρωση των νέων υπαλλήλων σε θέματα ασφάλειας πληροφοριών θα πρέπει να αποτελεί μέρος των αρχικών ενημερωτικών συναντήσεων/ενημερώσεων.

2.7 Έκδοση υλικού πληροφόρησης

Ο Υπεύθυνος Ασφάλειας Πληροφοριών σε συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων θα πρέπει να μεριμνούν για την περιοδική και όποτε απαιτείται έκδοση κατάλληλου υλικού ενημέρωσης, ώστε να υπενθυμίζουν σε όλους τους εμπλεκόμενους χρήστες τις ευθύνες τους σχετικά με την ασφάλεια πληροφοριών και την προστασία δεδομένων προσωπικού χαρακτήρα. Το Τμήμα Ανθρώπινου Δυναμικού (ΤΑΔ) της ΕΕΤΤ θα συνδράμει τις εν λόγω ενέργειες στο πλαίσιο των αρμοδιοτήτων του.

2.8 Σημεία επαφής για διευκρινίσεις

Το σημείο επαφής για διευκρινίσεις σχετικά με την ασφάλεια πληροφοριών είναι ο Υπεύθυνος Ασφάλειας Πληροφοριών και η Διεύθυνση Ψηφιακής Διακυβέρνησης.

2.9 Ευαισθητοποίηση τρίτων μερών

Η ΕΕΤΤ θα πρέπει να διασφαλίζει ότι οι εξωτερικοί συνεργάτες που χρησιμοποιούν τα πληροφοριακά συστήματά της, θα ενημερώνονται σχετικά με την Πολιτική Ασφάλειας της ΕΕΤΤ που είναι αναρτημένη στη Γνωσιακή Πύλη της.

2.10 Ευαισθητοποίηση σε ειδικά θέματα

Η ΕΕΤΤ οφείλει να ενημερώνει τους χρήστες σχετικά με:

- Τις συνέπειες των ενεργειών που θεωρούνται μη αποδεκτές (π.χ. μη εξουσιοδοτημένη χρήση των πληροφοριακών συστημάτων).
- Τους κινδύνους που προκύπτουν από κακόβουλο λογισμικό.
- Τους κινδύνους που απορρέουν από τη μη ασφαλή χρήση των αφαιρούμενων μέσων.
- Την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων.
- Την ιδιωτικότητα των επικοινωνιών και τη χρήση της κρυπτογραφίας.
- Το σύνολο των μηχανισμών παρακολούθησης που εφαρμόζονται από την ΕΕΤΤ στα πληροφοριακά συστήματα, προκειμένου να προστατεύεται η πρόσβαση, η διακίνηση και αποθήκευση ευαίσθητων ή κρίσιμων πληροφοριών.
- Το σύνολο των μηχανισμών που εφαρμόζονται από την ΕΕΤΤ για την προστασία των πληροφοριών, τόσο σε φυσικό, όσο και σε λογικό επίπεδο. Σε κάθε περίπτωση οι χρήστες θα πρέπει να γνωρίζουν τους σκοπούς συλλογής των πληροφοριών και τους ενδεδειγμένους τρόπους επεξεργασίας τους.
- Τα βήματα που θα πρέπει να ακολουθήσουν σε περιπτώσεις συμβάντων ασφάλειας, ώστε να μην καταστραφούν αποδεικτικά στοιχεία από υπολογιστές (π.χ. προσωπικούς υπολογιστές, φορητούς υπολογιστές, συσκευές δικτύωσης κτλ.).

- *Τις συνέπειες (σε νομικό επίπεδο ή / και σε επίπεδο ασφάλειας) που επιφέρει η εγκατάσταση, η χρήση και η τροποποίηση ελεύθερου λογισμικού ή λογισμικού ανοιχτού κώδικα.*

»

Β. Εντέλλεται την κοινοποίηση της παρούσας Απόφασης στο προσωπικό της ΕΕΤΤ μέσω ανάρτησής της στην Γνωσιακή Πύλη της ΕΕΤΤ (portal) και αποστολής της με μήνυμα ηλεκτρονικού ταχυδρομείου.

Γ. Ορίζει ότι η «Πολιτική Ενημέρωσης και Εκπαίδευσης Προσωπικού σε θέματα ασφάλειας πληροφοριών» συνδέεται άρρηκτα με την υπό στοιχείο 7. ως άνω «Πολιτική Ασφαλείας της ΕΕΤΤ» και πρέπει να εφαρμόζεται υποχρεωτικά και απαρέγκλιτα από το προσωπικό της ΕΕΤΤ και τους εξωτερικούς συνεργάτες που έχουν πρόσβαση στα πληροφοριακά συστήματα και την πληροφορία της (όπως φοιτητές που κάνουν πρακτική άσκηση ή ασκούμενοι δικηγόροι κτλ.).

Δ. Εξουσιοδοτεί τον Πρόεδρο της ΕΕΤΤ όπως:

- Προβεί σε κάθε διαδικαστική ενέργεια ή έκδοση πράξης, που θα διευκολύνει την έγκαιρη και πλήρη ολοκλήρωση κάθε δράσης που αφορά στην εφαρμογή της «Πολιτικής Ενημέρωσης και Εκπαίδευσης Προσωπικού σε θέματα ασφάλειας πληροφοριών».
- Τροποποιεί την «Πολιτική Ενημέρωσης και Εκπαίδευσης Προσωπικού σε θέματα ασφάλειας πληροφοριών» σε τακτική βάση σύμφωνα με τις ανάγκες της ΕΕΤΤ, προκειμένου να προσαρμόζεται στις εκάστοτε καταστάσεις, κινδύνους και περιορισμούς.

Ο ΠΡΟΕΔΡΟΣ

ΚΑΘΗΓΗΤΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ ΜΑΣΣΕΛΟΣ