ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

Μαρούσι, 27-03-2023

ΑΠ: 1069/13

ΑΠΟΦΑΣΗ

Έγκριση της «Πολιτικής Ασφάλειας Τελικού Χρήστη»

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),

Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

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,

4. Την ΑΠ 852/19/21-05-2018 Απόφαση της ΕΕΤΤ «*Ορισμός Υπευθύνου Προστασίας Δεδομένων της ΕΕΤΤ σύμφωνα με τον Κανονισμό (ΕΕ) 679/2016 (Γενικό Κανονισμό 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"*»,

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

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 Εισήγηση αριθ. 36705/21-03-2023 της αρμόδιας Υπηρεσίας της ΕΕΤΤ,

και ύστερα από προφορική εισήγηση του Προέδρου της ΕΕΤΤ (Καθηγητή Κωνσταντίνου Μασσέλου),

Επειδή :

Α. Τελικός χρήστης των συστημάτων πληροφορικής και επικοινωνιών της ΕΕΤΤ είναι ο κάθε υπάλληλος, συνεργάτης κτλ. της ΕΕΤΤ που χρησιμοποιεί τελικά ή προορίζεται να χρησιμοποιήσει τελικά τα συστήματα πληροφορικής και επικοινωνιών της ΕΕΤΤ. Ο όρος χρησιμοποιείται σε αντιδιαστολή προς το προσωπικό της ΕΕΤΤ που αναπτύσσει, συντηρεί ή υποστηρίζει αυτά τα συστήματα, όπως είναι ενδεικτικά οι διαχειριστές των συστημάτων.

Β. Οι τελικοί χρήστες οφείλουν να είναι όσο το δυνατόν περισσότερο ευαισθητοποιημένοι και ενημερωμένοι για την ασφάλεια πληροφοριών και υποδομών της ΕΕΤΤ και να συνεισφέρουν σε αυτήν. Για το λόγο αυτό, κρίνεται σκόπιμη η σύνταξη και γνωστοποίηση στο προσωπικό πολιτικής ασφάλειας τελικού χρήστη, η οποία θα εξειδικεύει, αναλύει και συμπληρώνει τις υπό στοιχείο 7. και 8. ως άνω πολιτικές, αναφορικά με τη χρήση των συστημάτων πληροφορικής και επικοινωνιών της ΕΕΤΤ από τους τελικούς χρήστες τους.

Αποφασίζει :

Α. **Εγκρίνει** την «Πολιτική Ασφάλειας Τελικού Χρήστη», η οποία καθορίζει τις αρχές και τους κανόνες σύμφωνα με τους οποίους πρέπει να γίνεται η χρήση των συστημάτων πληροφορικής και επικοινωνιών της ΕΕΤΤ, ώστε να διασφαλίζεται η ασφάλεια των πληροφοριών της. Η «Πολιτική Ασφάλειας Τελικού Χρήστη» έχει ως εξής:

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

«

Πολιτική Ασφάλειας Τελικού Χρήστη

Έκδοση: 1η

Τελευταία Ημερομηνία Ενημέρωσης: Μάρτιος 2023

1 Σκοπός και πεδίο εφαρμογής

Τελικός χρήστης των συστημάτων πληροφορικής και επικοινωνιών της ΕΕΤΤ είναι ο κάθε υπάλληλος, συνεργάτης κτλ. της ΕΕΤΤ που χρησιμοποιεί τελικά ή προορίζεται να χρησιμοποιήσει τελικά τα συστήματα πληροφορικής και επικοινωνιών της ΕΕΤΤ. Ο όρος χρησιμοποιείται σε αντιδιαστολή με το προσωπικό της ΕΕΤΤ που αναπτύσσει, συντηρεί ή υποστηρίζει αυτά τα συστήματα, όπως είναι ενδεικτικά οι διαχειριστές των συστημάτων. Οι τελικοί χρήστες οφείλουν να συνεισφέρουν στην ασφάλεια πληροφοριών και υποδομών της ΕΕΤΤ.

Σκοπός της πολιτικής ασφάλειας τελικού χρήστη είναι να καθορίσει τις αρχές και τους κανόνες σύμφωνα με τους οποίους πρέπει να γίνεται η χρήση των συστημάτων πληροφορικής και επικοινωνιών ώστε να διασφαλίζεται η ασφάλεια των πληροφοριών της ΕΕΤΤ, καθώς και να τους γνωστοποιήσει σε όλους τους χρήστες της.

Η παρούσα πολιτική εξειδικεύει και συμπληρώνει την Πολιτική Ασφαλείας και την Πολιτική Αποδεκτής Χρήσης των Πληροφοριακών Αγαθών της ΕΕΤΤ, αναφορικά με την χρήση των συστημάτων πληροφορικής και επικοινωνιών της ΕΕΤΤ από τους τελικούς χρήστες τους.

2 Ορθή χρήση των πληροφοριακών συστημάτων της ΕΕΤΤ

2.1 Βασικές αρχές

Οι βασικές αρχές που διέπουν την χρήση των πληροφοριακών συστημάτων της ΕΕΤΤ από τους τελικούς χρήστες συνοψίζονται στα εξής:

- *Η χρήση των συστημάτων πληροφορικής και επικοινωνιών της ΕΕΤΤ πραγματοποιείται μόνο για νόμιμους σκοπούς και με νόμιμο τρόπο και σύμφωνα με τις ειδικότερες οδηγίες και εγχειρίδια χρήσης του κάθε συστήματος.*
- *Αποτελεί υποχρέωση του κάθε χρήστη να χειρίζεται και να χρησιμοποιεί τον κάθε είδους εξοπλισμό συστημάτων ή δικτύου που ανήκει στην ΕΕΤΤ με αυξημένη προσοχή ώστε να μην προκαλούνται κλοπές, ζημιές ή φθορές. Τυχόν ατυχήματα θα πρέπει να αναφέρονται άμεσα στην Διεύθυνση Ψηφιακής Διακυβέρνησης ώστε να αποκαθίστανται το συντομότερο δυνατό.*
- *Η χρήση των υπολογιστικών και δικτυακών πόρων πρέπει να είναι λελογισμένη ώστε να μην δημιουργεί συνθήκες που σπαταλούν άσκοπα πόρους ή εν γένει να μην προκαλούν δυσλειτουργία.*
- *Οι χρήστες πρέπει να αναφέρουν οποιαδήποτε περίπτωση δυσλειτουργίας των συστημάτων που χρησιμοποιούν, αμέσως μόλις κάτι τέτοιο περιέλθει στην αντίληψή τους.*
- *Η πρόσβαση στα πληροφοριακά συστήματα είναι προνόμιο και όχι δικαίωμα. Αυτό σημαίνει ότι η πρόσβαση παρέχεται ρητά και σύμφωνα με τον κανόνα απόδοσης των ελάχιστων προνομίων (least privilege rule), διαφορετικά απορρίπτεται εξ' ορισμού. Σύμφωνα με τον κανόνα αυτό, στον κάθε χρήστη παρέχονται τα ελάχιστα δικαιώματα πρόσβασης που είναι απαραίτητα για την εκτέλεση των υπηρεσιακών καθηκόντων του.*
- *Η μη εξουσιοδοτημένη πρόσβαση στα πληροφοριακά συστήματα απαγορεύεται.*
- *Η πρόσβαση στα συστήματα της ΕΕΤΤ παρέχεται μόνο προς χρήση για υπηρεσιακούς σκοπούς. Η χρήση τους για προσωπικούς λόγους απαγορεύεται ρητά.*

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

- *Οι πληροφορίες της ΕΕΤΤ χρησιμοποιούνται μόνο για υπηρεσιακούς σκοπούς. Χρήση πληροφοριών της ΕΕΤΤ για διαφορετικούς σκοπούς επιτρέπεται μόνο κατόπιν ρητής έγκρισης.*
- *Οι πληροφορίες της ΕΕΤΤ μεταδίδονται μόνο σε εξουσιοδοτημένους χρήστες και με ασφαλείς τρόπους για την ελαχιστοποίηση των κινδύνων διαρροής τους.*
- *Η χρήση του Διαδικτύου και του υπηρεσιακού ηλεκτρονικού ταχυδρομείου γίνεται με αυξημένη προσοχή και με τρόπο που δεν αντιβαίνει στον υπηρεσιακό ρόλο τους αλλά σέβεται το κύρος της ΕΕΤΤ.*
- *Οι χρήστες δεν προβαίνουν σε ενέργειες που συνιστούν προσπάθεια παραβίασης ή υποβάθμισης (επιτυχούς ή μη) της ασφάλειας ή της ακεραιότητας των συστημάτων.*
- *Οι τελικοί χρήστες είναι υπεύθυνοι αναφορικά με την χρήση των συστημάτων της ΕΕΤΤ και οφείλουν να συμμορφώνονται με τις πολιτικές και διαδικασίες ασφαλείας της.*

Οι παραπάνω βασικές αρχές αναλύονται στα παρακάτω κεφάλαια της παρούσας πολιτικής.

2.2 Ενημέρωση και υποστήριξη των χρηστών

Οι χρήστες των συστημάτων πληροφορικής και επικοινωνιών της ΕΕΤΤ οφείλουν να είναι ενήμεροι και να συμμορφώνονται με την παρούσα Πολιτική Ασφάλειας Τελικού Χρήστη. Σε περίπτωση που απαιτείται βοήθεια για την κατανόηση ή/και την εφαρμογή της, οι χρήστες πρέπει να επικοινωνούν με την Διεύθυνση Ψηφιακής Διακυβέρνησης.

2.3 Ευθύνη των χρηστών για την αναφορά συμβάντων ασφαλείας

Η ΕΕΤΤ λαμβάνει μέριμνα για παροχή ικανοποιητικού επιπέδου ασφαλείας προς τους χρήστες. Όμως, παρά τα οργανωτικά και τεχνικά μέτρα που λαμβάνονται, δεν μπορεί να αποκλεισθεί η πιθανότητα παραβίασης της ασφάλειας των συστημάτων. Όπως άλλωστε ισχύει διεθνώς, κανένα ηλεκτρονικό δίκτυο δεν είναι απολύτως ασφαλές.

Οι χρήστες πρέπει να ενημερώνουν την Διεύθυνση Ψηφιακής Διακυβέρνησης για όποιο κενό ασφάλειας υποπέσει στην αντίληψή τους ή οποιαδήποτε ενέργεια, συμβάν ή δραστηριότητα παρατηρήσουν, η οποία συνιστά ή ενδέχεται να συνιστά μη αποδεκτή ή παράτυπη ενέργεια ή παραβίαση της ασφάλειας (όπως διαρροή πληροφοριών) της ΕΕΤΤ. Σε περίπτωση υποψίας, αμφιβολίας ή διαπίστωσης συμβάντος ή τρωτότητας, πρέπει να ειδοποιούν άμεσα την Διεύθυνση Ψηφιακής Διακυβέρνησης με όσες πληροφορίες διαθέτουν.

Η ΕΕΤΤ δεσμεύεται για την ενδελεχή διερεύνηση τέτοιων περιστατικών, τον εντοπισμό των υπευθύνων και την συνολική διαχείριση μέσω της Πολιτικής Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών που έχει υιοθετήσει.

2.4 Εμπιστευτικότητα και συμμόρφωση με την προστασία προσωπικών δεδομένων και την ιδιωτικότητα

Οι χρήστες οφείλουν να τηρούν εχεμύθεια για πληροφορίες που λαμβάνουν γνώση ή επεξεργάζονται κατά την χρήση των πληροφοριακών συστημάτων της ΕΕΤΤ στο πλαίσιο της εκτέλεσης των καθηκόντων τους και οι οποίες χαρακτηρίζονται απόρρητες από τις κείμενες διατάξεις ή όταν αυτό επιβάλλεται από την κοινή πείρα και λογική.

Όλοι οι χρήστες είναι υπεύθυνοι και οφείλουν να διασφαλίζουν το απόρρητο των επικοινωνιών και να συμμορφώνονται με τις απαιτήσεις που σχετίζονται με την προστασία προσωπικών δεδομένων. Όταν απαιτείται, πρέπει να συμβουλεύονται τον Υπεύθυνο Προστασίας Δεδομένων (DPO, DPO@eett.gr) ή τη Συμβουλευτική ομάδα προστασίας δεδομένων (Ομάδα GDPR, GDPR@eett.gr), σχετικά με τον τρόπο με τον οποίο θα χειρίζονται τα προσωπικά δεδομένα, καθώς και τις ευθύνες που έχουν έναντι αυτών.

2.5 Παρακολούθηση/Επίβλεψη της ορθής και ασφαλούς χρήσης

Η ΕΕΤΤ διατηρεί το δικαίωμα, μέσω εξουσιοδοτημένων στελεχών της, να παρακολουθεί την δραστηριότητα των χρηστών των συστημάτων πληροφορικής και επικοινωνιών της στο πλαίσιο της εκτέλεσης των υπηρεσιακών καθηκόντων τους, προκειμένου να επαληθεύει την ορθή και ασφαλή χρήση των συστημάτων της.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

Οι χρήστες πρέπει να γνωρίζουν ότι οποιαδήποτε ενέργεια (όπως καταχώρηση, μεταβολή, διαγραφή, εμφάνιση, εκτύπωση κτλ. στοιχείων) που πραγματοποιείται στα πληροφοριακά συστήματα της ΕΕΤΤ, δύναται να καταγράφεται και να τηρείται, και μπορεί να αποδοθεί στο άτομο που την εκτέλεσε.

2.6 Μη εξουσιοδοτημένες απόπειρες πρόσβασης

Οι χρήστες απαγορεύεται να προβαίνουν σε εκμετάλλευση πιθανών κενών ασφαλείας του τηλεπικοινωνιακού εξοπλισμού, των συστημάτων, υπηρεσιών και εφαρμογών της ΕΕΤΤ, σε διατάραξη της ομαλής λειτουργίας τους ή σε εκτέλεση οποιουδήποτε κακόβουλου λογισμικού ή οποιασδήποτε άλλης ενέργειας που ενδέχεται να θέσει σε κίνδυνο ή να υποβαθμίσει το επίπεδο ασφάλειας των συστημάτων της ΕΕΤΤ.

Απαγορεύεται ρητά οποιαδήποτε απόπειρα παράκαμψης των μηχανισμών ελέγχου πρόσβασης και προστασίας που εφαρμόζονται στα πληροφοριακά συστήματα, η οποία γίνεται με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης.

Οι χρήστες δεν επιτρέπεται να υποκλέπτουν ή να αποκτούν με οποιονδήποτε άλλο τρόπο, κωδικούς πρόσβασης, κρυπτογραφικά κλειδιά ή οποιοδήποτε άλλο μηχανισμό ελέγχου πρόσβασης, ο οποίος θα διευκόλυνε τη μη εξουσιοδοτημένη πρόσβασή τους σε τέτοια συστήματα.

2.7 Πρόσβαση σε αρχεία άλλων χρηστών

Οι χρήστες δεν πρέπει να αποκτούν πρόσβαση, να διαβάζουν, να τροποποιούν, να διαγράφουν ή να αντιγράφουν αρχεία που ανήκουν σε άλλο χρήστη, χωρίς να έχουν λάβει προηγούμενη άδεια. Η κατοχή δε ενός τέτοιου προνομίου δεν δίνει δικαίωμα σε κανένα χρήστη να αποκτά πρόσβαση σε ξένες πληροφορίες, παρά μόνο κατόπιν ρητής έγκρισης.

Επιπλέον, απαγορεύεται η δημιουργία και χρήση κοινόχρηστων φακέλων και αρχείων σε υπολογιστή χρήστη, καθώς και η χρήση λύσεων ηλεκτρονικής ανταλλαγής και αποθήκευσης δεδομένων, εφόσον δεν είναι εγκεκριμένες από την ΕΕΤΤ. Σε περίπτωση που προκύψει ανάγκη για κοινή χρήση δεδομένων, οι χρήστες πρέπει να απευθύνονται στην Διεύθυνση Ψηφιακής Διακυβέρνησης.

2.8 Εγκατάσταση και τροποποίηση λογισμικού και υλικού

Η μη εξουσιοδοτημένη εγκατάσταση ή τροποποίηση λογισμικού ή/και υλικού απαγορεύεται.

Οποιεσδήποτε αλλαγές στα υφιστάμενα πληροφοριακά συστήματα πρέπει να πραγματοποιούνται μόνο από εξουσιοδοτημένα άτομα, σύμφωνα με τις πολιτικές και διαδικασίες της ΕΕΤΤ ή τις σχετικές συμφωνίες με τους αναδόχους.

2.9 Χρήση πληροφοριακών συστημάτων από μη εργαζόμενους στην ΕΕΤΤ

Τα πληροφοριακά συστήματα της ΕΕΤΤ δεν επιτρέπεται να χρησιμοποιούνται από μη εγκεκριμένα άτομα (π.χ. τρίτους, μέλη της οικογένειας των εργαζομένων κτλ.), εκτός εάν αυτά έχουν λάβει ρητή εξουσιοδότηση.

2.10 Χρήση πληροφοριακών συστημάτων και εξοπλισμού που παρέχεται από τρίτη οντότητα

Οι χρήστες επιτρέπεται να χρησιμοποιούν πληροφοριακά συστήματα και εξοπλισμό που δεν ανήκει στην ΕΕΤΤ (π.χ. προσωπικούς φορητούς υπολογιστές, κινητά τηλέφωνα κτλ.) εντός των εγκαταστάσεών της, υπό την προϋπόθεση ότι δεν συνδέονται στο δίκτυο της ΕΕΤΤ. Η σύνδεση στο δίκτυο της ΕΕΤΤ γίνεται αποκλειστικά, κατόπιν ρητής εξουσιοδότησης, από την Διεύθυνση Ψηφιακής Διακυβέρνησης.

2.11 Περιορισμένη προσωπική χρήση των πληροφοριακών συστημάτων της ΕΕΤΤ

Τα πληροφοριακά συστήματα της ΕΕΤΤ είναι ιδιοκτησία της και παρέχονται στους εργαζόμενους για την εκτέλεση των εργασιών της. Ως εκ τούτου, η χρήση τους θα πρέπει να γίνεται για υπηρεσιακούς σκοπούς. Η περιστασιακή χρήση των πληροφοριακών συστημάτων της ΕΕΤΤ για προσωπικούς σκοπούς επιτρέπεται μόνο κατόπιν ρητής εξουσιοδότησης. Η προσωπική χρήση των πληροφοριακών συστημάτων της ΕΕΤΤ συνιστά προνόμιο και όχι δικαίωμα, ενώ η κατάχρηση αυτού του προνομίου, μπορεί να οδηγήσει σε ανάκληση ή/και πειθαρχική ή άλλη νομική ενέργεια.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

Η προσωπική χρήση των πληροφοριακών πόρων της ΕΕΤΤ πρέπει να συμμορφώνεται με την παρούσα Πολιτική Ασφάλειας Τελικού Χρήστη. Συγκεκριμένα, οι χρήστες πρέπει να διασφαλίζουν ότι η προσωπική χρήση:

- *δεν θα έχει ως αποτέλεσμα την οποιουδήποτε είδους απώλεια για την ΕΕΤΤ,*
- *δεν αποσκοπεί σε προσωπικό όφελος του χρήστη ή οποιασδήποτε άλλης τρίτης επιχειρησιακής οντότητας,*
- *δεν καταναλώνει σημαντικούς πόρους από τα συστήματα,*
- *δεν επηρεάζει την παραγωγικότητα των εργαζομένων,*
- *δεν ενοχλεί τους συναδέλφους και δεν προκαλεί συγκρούσεις,*
- *δεν έχει ως αποτέλεσμα κακόβουλες ή παράνομες δραστηριότητες,*
- *δεν παραβιάζει οποιαδήποτε άλλη πολιτική της ΕΕΤΤ.*

Η ΕΕΤΤ διατηρεί το δικαίωμα να αποφασίσει τι συνιστά εκτεταμένη (και επομένως μη αποδεκτή) προσωπική χρήση.

2.12 Αντίγραφα ασφάλειας (backup) δεδομένων τελικού χρήστη

Η Διεύθυνση Ψηφιακής Διακυβέρνησης είναι υπεύθυνη για την λήψη αντιγράφων ασφαλείας του συνόλου των κεντρικών συστημάτων της ΕΕΤΤ με στόχο την συνέχεια της λειτουργίας της σε περίπτωση οποιασδήποτε αποτυχίας. Η Διεύθυνση Ψηφιακής Διακυβέρνησης δεν είναι υπεύθυνη για την λήψη αντιγράφων ασφαλείας των δεδομένων των χρηστών όσο αυτά βρίσκονται στους προσωπικούς τους υπολογιστές. Κάθε χρήστης, όμως, έχει έναν προσωπικό χώρο στον File Server[1] της ΕΕΤΤ, όπου μπορεί να αποθηκεύσει ότι κρίνει απαραίτητο για την εργασία του. Για τα δεδομένα του File Server λαμβάνονται αντίγραφα ασφαλείας από την Διεύθυνση Ψηφιακής Διακυβέρνησης.

Επομένως, οι ίδιοι οι χρήστες καθίστανται υπεύθυνοι για τον προγραμματισμό και την εκτέλεση της αποθήκευσης των κρίσιμων δεδομένων τους στον File Server, σε τακτά χρονικά διαστήματα.

Για περισσότερες πληροφορίες ή/και βοήθεια, οι χρήστες πρέπει να ανατρέξουν στην Πολιτική Ασφαλείας της ΕΕΤΤ ή εναλλακτικά να επικοινωνήσουν με την Διεύθυνση Ψηφιακής Διακυβέρνησης.

3 Ορθή χρήση φορητών υπολογιστών, φορητών συσκευών και αφαιρούμενων μέσων

3.1 Χρήση, αποθήκευση και μεταφορά φορητών υπολογιστών και φορητών συσκευών

Οι χρήστες της ΕΕΤΤ είναι υπεύθυνοι για την προστασία των φορητών συσκευών που χρησιμοποιούν για την πρόσβαση σε συστήματα και πληροφορίες της, είτε οι συσκευές αυτές παρέχονται από την ΕΕΤΤ, είτε αποτελούν προσωπικά αγαθά.

Οι φορητοί υπολογιστές και οι φορητές συσκευές πρέπει να προστατεύονται από τους εξουσιοδοτημένους χρήστες τους σύμφωνα με το επίπεδο διαβάθμισης των πληροφοριών και δεδομένων που περιέχουν, όπως προβλέπεται στις πολιτικές ασφάλειας της ΕΕΤΤ.

Πρέπει να αποθηκεύονται με ασφάλεια εντός ελεγχόμενων περιοχών και σύμφωνα με το ισχύον επίπεδο διαβάθμισής τους.

Οι κωδικοί πρόσβασης των φορητών συσκευών δεν πρέπει να διατηρούνται μαζί με τη συσκευή που προστατεύουν.

Σε κάθε περίπτωση, οι χρήστες πρέπει να λαμβάνουν όλα τα απαραίτητα μέτρα, προκειμένου κακόβουλο λογισμικό να μην μολύνει τους φορητούς υπολογιστές ή/και τις φορητές συσκευές τους.

Οι συσκευές αυτού του είδους πρέπει να προστατεύονται και όταν μεταφέρονται εκτός του χώρου της ΕΕΤΤ, χρησιμοποιώντας τα κατάλληλα φυσικά και λογικά μέτρα ασφάλειας, π.χ. κλειδωμένος χώρος φύλαξης,

[1] File server είναι ένας υπολογιστής υπεύθυνος για την αποθήκευση και διαχείριση αρχείων δεδομένων, έτσι ώστε άλλοι υπολογιστές στο ίδιο δίκτυο να έχουν πρόσβαση στα αρχεία αυτά.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

κρυπτογράφηση, προστασία της οθόνης και του πληκτρολογίου της συσκευής όταν χρησιμοποιείται από την οπτική επαφή τρίτων (shoulder surfing) κτλ.

Δεν πρέπει να παραμένουν χωρίς επιτήρηση σε δημόσιους χώρους. Εάν αυτό δεν είναι εφικτό, τότε δεν θα πρέπει να βρίσκονται σε ορατό σημείο. Κατά την διάρκεια ενός υπηρεσιακού ταξιδιού, οι φορητές συσκευές πρέπει να μεταφέρονται ως χειραποσκευές.

Οι χρήστες δεν πρέπει να αφήνουν τις συσκευές τους ξεκλείδωτες κατά το χρονικό διάστημα που αυτές δεν βρίσκονται υπό την επιτήρησή τους. Αυτές πρέπει να κλειδώνουν, να αποσυνδέεται ο χρήστης ή να χρησιμοποιούν οθόνη προστασίας με χρήση κωδικού πρόσβασης.

Η απώλεια φορητών συσκευών που χρησιμοποιούνται για υπηρεσιακούς σκοπούς της ΕΕΤΤ πρέπει να δηλώνεται άμεσα.

3.2 Χρήση, αποθήκευση και μεταφορά αφαιρούμενων μέσων

Οι υπάλληλοι της ΕΕΤΤ πρέπει να χρησιμοποιούν αφαιρούμενα μέσα αποκλειστικά σύμφωνα με τις πολιτικές ασφαλείας της ΕΕΤΤ.

Τα αφαιρούμενα μέσα πρέπει να προστατεύονται από τους εξουσιοδοτημένους χρήστες τους σύμφωνα με το επίπεδο διαβάθμισης των πληροφοριών και δεδομένων που περιέχουν.

Πριν την χρήση, τα αφαιρούμενα μέσα πρέπει πρώτα να σαρώνονται για κακόβουλο λογισμικό.

Η χρήση αφαιρούμενων μέσων που είναι άγνωστης προέλευσης απαγορεύεται.

Παράλληλα, τα αφαιρούμενα μέσα δεν πρέπει να συνδέονται με συστήματα που δεν ανήκουν στην ΕΕΤΤ, εκτός εάν οι χρήστες τους έχουν εξουσιοδοτηθεί ρητά να το πράξουν. Σε αυτή την περίπτωση, πρέπει να δοθεί ιδιαίτερη προσοχή προκειμένου να διασφαλιστεί ότι τα αφαιρούμενα μέσα δεν θα μολυνθούν από κακόβουλο λογισμικό.

Η ΕΕΤΤ διατηρεί το δικαίωμα να απενεργοποιήσει την σύνδεση αφαιρούμενων μέσων.

Τα αφαιρούμενα μέσα πρέπει να αποθηκεύονται με ασφάλεια από τον εξουσιοδοτημένο χρήστη τους εντός ελεγχόμενων περιοχών και σύμφωνα με το ισχύον επίπεδο διαβάθμισής τους.

Όλα τα αφαιρούμενα μέσα πρέπει να προστατεύονται όταν απομακρύνονται από τους χώρους της ΕΕΤΤ, χρησιμοποιώντας τα κατάλληλα φυσικά και λογικά μέτρα ασφάλειας, π.χ. κλειδωμένος χώρος φύλαξης, κατάλληλη συσκευασία, κρυπτογράφηση, αξιόπιστη μεταφορά με χρήση courier, να μην αφήνονται χωρίς επιτήρηση σε δημόσιους χώρους κτλ.

Σε κάθε περίπτωση, οι εξουσιοδοτημένοι χρήστες των αφαιρούμενων μέσων της ΕΕΤΤ πρέπει να λαμβάνουν όλα τα απαραίτητα μέτρα προκειμένου να αποτρέψουν μόλυνση από κακόβουλο λογισμικό.

3.3 Απομακρυσμένη πρόσβαση και εξ αποστάσεως εργασία

Η απομακρυσμένη πρόσβαση στα πληροφοριακά συστήματα της ΕΕΤΤ από τους χρήστες και η εξ αποστάσεως εργασία διεξάγεται σύμφωνα με την Πολιτική Τηλεργασίας και Φορητών Συσκευών της ΕΕΤΤ.

Αποτελεί συνειδητή πολιτική της ΕΕΤΤ η παροχή υπηρεσιακών φορητών υπολογιστών στο σύνολο του προσωπικού που τηλεργάζεται. Για λόγους ασφαλείας, στόχος είναι ο περιορισμός στο ελάχιστο δυνατό και η εν τέλει εξάλειψη της χρήσης ιδιόκτητων υπολογιστών (Bring Your Own Device – B.Y.O.D.).

Για την σύνδεσή τους στο Διαδίκτυο μέσω του οικιακού ασύρματου δικτύου (Wi-Fi), οι χρήστες πρέπει να χρησιμοποιούν ασφαλές πρωτόκολλο Wi-Fi Protected Access II (WPA2) ή Wi-Fi Protected Access III (WPA3) και ισχυρούς κωδικούς πρόσβασης (passwords).

Για τις τηλεδιασκέψεις πρέπει να χρησιμοποιούν την τελευταία έκδοση εγκεκριμένης εφαρμογής τηλεδιάσκεψης με ρύθμιση που θα εγκαθιστά με αυτοματοποιημένο τρόπο τις ενημερώσεις (updates). Δεν πρέπει να ορίζουν τις τηλεδιασκέψεις ως δημόσιες (public), εκτός αν υπάρχει λόγος γι' αυτό. Όπου απαιτείται, πρέπει να χρησιμοποιούν ισχυρούς κωδικούς (meeting codes και passwords) για κάθε τηλεδιάσκεψη και να μην τους ξαναχρησιμοποιούν. Επίσης, δεν πρέπει να αναρτούν τον σύνδεσμο (link) της τηλεδιάσκεψης σε δημόσια

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

διαθέσιμο ιστότοπο (π.χ. social media post). Το link και οι κωδικοί θα πρέπει να αποστέλλονται κατ' ευθείαν στους αποδέκτες (π.χ. με email ή instant messaging).

Για λόγους προστασίας της ιδιωτικότητας και της ασφάλειας, συνιστάται οι χρήστες να αποσυνδέουν την web camera από τον υπολογιστή όταν δεν την χρησιμοποιούν, να την απενεργοποιούν ή να την καλύπτουν στην περίπτωση ενσωματωμένης web camera.

Στην περίπτωση που ο τηλεργαζόμενος χρησιμοποιεί B.Y.O.D., πρέπει να:

- *χρησιμοποιεί έναν ξεχωριστό λογαριασμό χρήστη με ελάχιστα προνόμια (non-privileged). Γενικά, να χρησιμοποιεί διαχειριστικό λογαριασμό μόνο για εργασίες συντήρησης του οικιακού του υπολογιστή, καθώς και για εγκατάσταση προγραμμάτων και ενημερώσεων*
- *χρησιμοποιείται η πλέον πρόσφατη και υποστηριζόμενη έκδοση για το λειτουργικό σύστημα και τις εφαρμογές και να ενεργοποιείται η αυτόματη εγκατάσταση ενημερώσεων*
- *εγκαθίσταται στον οικιακό υπολογιστή αντιικό λογισμικό[2] (antivirus), το οποίο θα λαμβάνει ενημερώσεις με αυτόματο τρόπο και θα παρέχει επιπλέον υπηρεσίες ασφαλείας (anti-phishing[3], anti-malware[4], ασφαλή πλοήγηση και δυνατότητες firewall[5])*
- *μην πραγματοποιεί λήψη περιεχομένου από το διαδίκτυο*
- *προβαίνει τακτικά σε λήψη αντιγράφων ασφαλείας (backup) των αρχείων στον file server της ΕΕΤΤ ώστε να ελαχιστοποιεί την απειλή μόλυνσης από ransomware[6]*

Αναφορικά με τη χρήση μη ασφαλών ή ανοικτών ασύρματων δικτύων (public Wi-Fi hot spots), οι χρήστες πρέπει:

- *όσο είναι εφικτό, να αποφεύγουν την άμεση χρήση public Wi-Fi hot spots και ιδιαίτερα για την είσοδο σε ευαίσθητους λογαριασμούς (π.χ. web banking)*
- *να προτιμούν την δημιουργία δικού τους hot spot μέσω του δικτύου κινητής τηλεφωνίας της συσκευής τους και με την χρήση ισχυρού κωδικού (password)*
- *εφόσον επιβάλλεται από τις συνθήκες η χρήση public Wi-Fi hot spot, να χρησιμοποιούν την υπηρεσία VPN (Virtual Private Network) της ΕΕΤΤ γιατί η συγκεκριμένη επιλογή θα τους προστατέψει από παρακολούθηση και άλλες κακόβουλες δραστηριότητες.*

---

[2] Ιός υπολογιστή είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να «μολύνει» τον υπολογιστή χωρίς την γνώση ή την άδεια του χρήστη του. Αντιικό λογισμικό είναι το λογισμικό προστασίας από ιούς, δηλαδή ένα πρόγραμμα υπολογιστή που χρησιμοποιείται για την πρόληψη, τον εντοπισμό, και την αφαίρεση των ιών.

[3] Phishing είναι ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο "θύτης" υποδύεται μία αξιόπιστη οντότητα, καταχρώμενος την ελλιπή προστασία που παρέχουν τα ηλεκτρονικά εργαλεία και την άγνοια του χρήστη-"θύματος", με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων, όπως είναι ευαίσθητα ιδιωτικά στοιχεία και κωδικοί. Το λογισμικό κατά του phishing (anti-phishing) αποτελείται από προγράμματα υπολογιστών που προσπαθούν να αναγνωρίσουν περιεχόμενο phishing που περιέχεται σε ιστοτόπους, e-mail ή άλλες φόρμες που χρησιμοποιούνται για την πρόσβαση σε δεδομένα (συνήθως από το διαδίκτυο) και αποκλείουν το περιεχόμενο phishing, συνήθως με μια προειδοποίηση προς τον χρήστη (και συχνά μια επιλογή για προβολή του περιεχομένου).

[4] Malware ή κακόβουλο λογισμικό είναι οποιοδήποτε λογισμικό που έχει σκόπιμα σχεδιαστεί για να προκαλέσει διαταραχή σε έναν υπολογιστή, διακομιστή, ή δίκτυο υπολογιστών, να διαρρεύσει προσωπικές πληροφορίες, να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες και συστήματα, να στερεί την πρόσβαση στον χρήστη σε πληροφορίες ή να παρεμβαίνει εν αγνοία του στην ασφάλεια και το απόρρητο του υπολογιστή του. Το λογισμικό κατά του malware (anti-malware) είναι ένα πρόγραμμα υπολογιστή που χρησιμοποιείται για την πρόληψη, τον εντοπισμό και την αφαίρεση κακόβουλου λογισμικού.

[5] Firewall ή τείχος προστασίας είναι μια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο.

[6] Το ransomware είναι ένα είδος κακόβουλου λογισμικού που απειλεί να δημοσιοποιήσει τα προσωπικά δεδομένα του θύματος ή να διακόψει την πρόσβασή του θύματος στα αρχεία του, μέχρι να δοθούν λύτρα από το θύμα.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

4 Λογισμικό

4.1 Χρήση πληροφοριακών συστημάτων και εφαρμογών της ΕΕΤΤ

Το παρόν αφορά όλα τα πληροφοριακά συστήματα και εφαρμογές που χρησιμοποιεί η ΕΕΤΤ, δηλαδή τα εσωτερικά ανεπτυγμένα, τα εξωτερικά ανεπτυγμένα, τα λογισμικά πακέτα έτοιμα προς χρήση, τα πληροφοριακά συστήματα τρίτων στα οποία έχει πρόσβαση η ΕΕΤΤ κτλ.

Οι χρήστες πρέπει να συμμορφώνονται με τους κανόνες λειτουργίας των εγχειριδίων χρήσης των συστημάτων και εφαρμογών που χρησιμοποιούν. Για υποστήριξη πρέπει να απευθύνονται στην Διεύθυνση Ψηφιακής Διακυβέρνησης.

4.2 Προστασία προσωπικών δεδομένων των χρηστών των συστημάτων

Προσωπικά δεδομένα που ζητούνται για την εξακρίβωση της ταυτότητας των χρηστών που ζητούν πρόσβαση στα πληροφοριακά συστήματα και τις εφαρμογές της ΕΕΤΤ, χρησιμοποιούνται αποκλειστικά και μόνο για την επαλήθευση της ταυτότητάς τους και δεν υπόκεινται σε άλλη επεξεργασία. Περισσότερες πληροφορίες είναι διαθέσιμες στη "Δήλωση προστασίας προσωπικών δεδομένων» στον διαδικτυακό τόπο της ΕΕΤΤ, που εξηγεί τα είδη των προσωπικών δεδομένων που τηρεί η ΕΕΤΤ και τους τρόπους που τα συλλέγει, χρησιμοποιεί, διαχειρίζεται και προστατεύει, καθώς και τα δικαιώματα των υποκειμένων των δεδομένων.

4.3 Άδειες χρήσης λογισμικού

Οι χρήστες θα πρέπει να χειρίζονται οποιοδήποτε λογισμικό αυστηρά σύμφωνα με τους όρους της συγκεκριμένης άδειας χρήσης. Συγκεκριμένα, απαγορεύεται οποιοσδήποτε τύπος χρήσης ή αντιγραφής λογισμικού που δεν συμμορφώνεται με τους όρους της άδειας χρήσης του.

Επιπλέον, οι χρήστες πρέπει να θεωρούν ότι κάθε είδους λογισμικό προστατεύεται από δικαιώματα πνευματικής ιδιοκτησίας, εκτός εάν υπάρχει σαφής ένδειξη που να δηλώνει το αντίθετο. Επομένως, πρέπει να προστατεύουν τα πνευματικά δικαιώματα και την πνευματική ιδιοκτησία.

4.4 Χρήση μη εγκεκριμένου λογισμικού

Η ΕΕΤΤ διατηρεί μία λίστα με τα εγκεκριμένα λογισμικά που μπορούν να εγκατασταθούν στα συστήματά της. Μη εγκεκριμένο λογισμικό δεν επιτρέπεται να χρησιμοποιείται, να εγκαθίσταται ή να αποθηκεύεται, εκτός εάν έχει δοθεί ρητή έγκριση. Η εγκατάσταση λογισμικού που δεν περιλαμβάνεται στην εν λόγω λίστα θα πρέπει να εξεταστεί και να εγκριθεί πριν πραγματοποιηθεί.

5 Διαχείριση Προσβάσεων στα πληροφοριακά συστήματα

5.1 Λογαριασμοί χρηστών

Τα πληροφοριακά συστήματα της ΕΕΤΤ επιβεβαιώνουν την ταυτότητα των χρηστών που συνδέονται σε αυτά, με ασφαλή μέθοδο.

Οι λογαριασμοί των χρηστών πρέπει να περιορίζουν την πρόσβαση/επεξεργασία μόνο στις πληροφορίες που είναι απαραίτητες για την εκτέλεση των καθηκόντων τους.

Οι λογαριασμοί χρήστη είναι αυστηρά προσωπικοί. Οι χρήστες των πληροφοριακών συστημάτων πρέπει να χρησιμοποιούν τους λογαριασμούς τους υπεύθυνα, αποκτώντας πρόσβαση στα πληροφοριακά συστήματα με χρήση του δικού τους λογαριασμού, αποφεύγοντας οποιαδήποτε ενέργεια με χρήση άλλου λογαριασμού.

Κάθε χρήστης είναι υπεύθυνος για τυχόν ενέργειες που πραγματοποιήθηκαν με χρήση του λογαριασμού του. Ωστόσο, σε περίπτωση που αποδειχθεί ότι ο λογαριασμός χρήστη έχει παραβιαστεί χωρίς αμέλεια ή δόλο από την πλευρά του χρήστη, αυτός/αυτή δεν θα θεωρείται υπεύθυνος.

Οι χρήστες πρέπει να ενημερώσουν αμελλητί την Διεύθυνση Ψηφιακής Διακυβέρνησης σε περίπτωση διαρροής στοιχείων του λογαριασμού τους.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

5.2 Διαχείριση κωδικών πρόσβασης

Οι χρήστες πρέπει να χρησιμοποιούν ισχυρούς κωδικούς πρόσβασης (passwords) σύμφωνα με τις πολιτικές της ΕΕΤΤ, δηλαδή κωδικούς που είναι δύσκολο να μαντέψει ένα άτομο ή πρόγραμμα, με ικανοποιητικό μήκος χαρακτήρων, με συνδυασμό κεφαλαίων και μικρών γραμμάτων, αριθμών και ειδικών χαρακτήρων και χωρίς ονόματα ή κοινές λέξεις που υπάρχουν σε λεξικά. Επίσης, πρέπει να χρησιμοποιούν διαφορετικό κωδικό για κάθε υπηρεσιακό ή προσωπικό λογαριασμό που διαθέτουν και να τους αλλάζουν τακτικά. Δεν πρέπει να χρησιμοποιούν τον ίδιο κωδικό πρόσβασης για συστήματα που ανήκουν σε εξωτερικά δίκτυα (π.χ. Διαδίκτυο) και σε συστήματα που ανήκουν στην ΕΕΤΤ.

Οι κωδικοί πρόσβασης που χρησιμοποιούνται στα πληροφοριακά συστήματα είναι αυστηρά προσωπικοί και χαρακτηρίζονται ως εμπιστευτική πληροφορία. Οι κωδικοί πρόσβασης δεν πρέπει ποτέ να είναι καταγεγραμμένοι ή αποθηκευμένοι σε μέρη προσβάσιμα από άλλους (π.χ. σε ένα κομμάτι χαρτί εκτεθειμένο πάνω στο πληκτρολόγιο). Δεν πρέπει να αποθηκεύονται σε ηλεκτρονική μορφή, να αποστέλλονται με ηλεκτρονικό ταχυδρομείο ούτε να αποκαλύπτονται σε τρίτους. Η επίδειξη και εκτύπωση των κωδικών πρόσβασης θα πρέπει να αποφεύγεται, αλλά σε περιπτώσεις που αυτό δεν είναι εφικτό, πρέπει να πραγματοποιείται με τέτοιο τρόπο ώστε να αποφεύγεται η αποκάλυψη κωδικών πρόσβασης σε μη εξουσιοδοτημένα μέρη.

Οι χρήστες είναι υπεύθυνοι να προστατεύουν τους κωδικούς πρόσβασής τους και να μην τους αποκαλύπτουν σε άλλους. Κάθε φορά που υπάρχει ανάγκη κοινής χρήσης δεδομένων, οι χρήστες πρέπει να επικοινωνούν με την Διεύθυνση Ψηφιακής Διακυβέρνησης, ενώ οι κωδικοί πρόσβασής τους δεν πρέπει ποτέ να διαμοιράζονται.

Οι χρήστες πρέπει να αποφεύγουν την αποθήκευση των κωδικών τους σε προγράμματα περιήγησης ιστού (web browser), σε εφαρμογές άμεσων μηνυμάτων (instant messaging applications) ή σε εφαρμογές ηλεκτρονικού ταχυδρομείου. Σε διαφορετική περίπτωση, μη εξουσιοδοτημένα άτομα που ενδέχεται να έχουν φυσική πρόσβαση στη συσκευή τους, θα μπορέσουν να αποκτήσουν πρόσβαση στο Διαδίκτυο και να διαβάσουν ή να στείλουν μηνύματα/e-mail χρησιμοποιώντας το λογαριασμό τους.

Οι χρήστες πρέπει να αλλάζουν αμέσως τον κωδικό πρόσβασης εάν τον μοιράστηκαν με κάποιον άλλο ή εάν πιστεύουν ότι έχει κλαπεί ή αποκαλυφθεί σε κάποιον άλλο.

Για την αποτελεσματικότερη διαχείριση των κωδικών πρόσβασης πρέπει να χρησιμοποιούνται ειδικά προγράμματα διαχείρισης κωδικών που προτείνονται από την Διεύθυνση Ψηφιακής Διακυβέρνησης.

Η διαχείριση των κωδικών πρόσβασης πρέπει να γίνεται σύμφωνα με την Πολιτική Ασφαλείας της ΕΕΤΤ.

5.3 Άρση ή τροποποίηση δικαιωμάτων πρόσβασης

Εάν κάποιος χρήστης διαπιστώσει ότι ο λογαριασμός του παρέχει δυνατότητες πρόσβασης /επεξεργασίας σε επιπλέον πληροφορίες από αυτές που απαιτούνται για την εκτέλεση των καθηκόντων του, οφείλει αμελλητί να ενημερώσει τον Προϊστάμενό του, ο οποίος πρέπει να επικοινωνήσει άμεσα με την Διεύθυνση Ψηφιακής Διακυβέρνησης προκειμένου να καταργηθούν τα επιπλέον δικαιώματα του λογαριασμού.

Σε κάθε περίπτωση οι Προϊστάμενοι πρέπει να ελέγχουν περιοδικά τα δικαιώματα του προσωπικού τους και να αιτούνται άμεσα στην Διεύθυνση Ψηφιακής Διακυβέρνησης τυχόν αλλαγές, διότι έχουν την ευθύνη της εξουσιοδότησης της πρόσβασης στα συστήματα και στις πληροφορίες της Διεύθυνσης / Τμήματός τους.

Η πρόσβαση των χρηστών στα συστήματα αίρεται με την λύση της εργασιακής σχέσης και τις μακροχρόνιες απουσίες ή προσαρμόζεται στις εκάστοτε αλλαγές. Επομένως, το Τμήμα Ανθρώπινου Δυναμικού πρέπει να ενημερώνει άμεσα την Διεύθυνση Ψηφιακής Διακυβέρνησης για τους νέους υπαλλήλους, φοιτητές που κάνουν πρακτική άσκηση, ασκούμενους δικηγόρους, για αποσπάσεις σε άλλες δημόσιες υπηρεσίες, εσωτερικές μετακινήσεις, μακροχρόνιες απουσίες, λύση εργασιακών σχέσεων, προκειμένου να προσαρμόζονται κατάλληλα οι προσβάσεις.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

6 Ορθή χρήση υπηρεσιών Διαδικτύου, ηλεκτρονικού ταχυδρομείου και μηνυμάτων

6.1 Γενική αρχή της εύλογης χρήσης

Αποτελεί γενική αρχή ότι η χρήση του Διαδικτύου και του υπηρεσιακού ηλεκτρονικού ταχυδρομείου πρέπει να γίνεται με τρόπο που δεν αντιβαίνει στον υπηρεσιακό ρόλο τους, δεν προσβάλλει το κύρος της ΕΕΤΤ και ακολουθεί τους κανόνες της δεοντολογίας και της ασφάλειας.

Επιπλέον, η χρήση των υπηρεσιών Διαδικτύου, ηλεκτρονικού ταχυδρομείου και μηνυμάτων πρέπει να γίνεται με εύλογο τρόπο, ώστε να αποφεύγεται η υπερφόρτωση των συστημάτων της ΕΕΤΤ και του δικτύου. Υπό αυτό το πρίσμα, απαγορεύεται η αποστολή/παραλαβή μαζικών μηνυμάτων, αλληλογραφίας αλυσίδας, μεγάλων αρχείων, αρχείων ήχου, βίντεο ή παρόμοιου τύπου αρχείων, καθώς και η εκτεταμένη περιήγηση στο Διαδίκτυο, εκτός εάν δοθεί σχετική ρητή έγκριση.

Σύμφωνα με τις πολιτικές της ΕΕΤΤ, κάθε χρήστης διαθέτει μέγιστο μέγεθος λαμβανομένων και αποστελλομένων μηνυμάτων και μέγιστο μέγεθος ταχυδρομικής θυρίδας. Τα εισερχόμενα μηνύματα που διακινούνται μέσω ηλεκτρονικού ταχυδρομείου ελέγχονται από ειδικό λογισμικό προστασίας κατά ιών πριν την παράδοσή τους.

6.2 Προσεκτική χρήση κατά την επίσκεψη σε ύποπτους ιστοτόπους

Οι χρήστες θα πρέπει να γνωρίζουν ότι υπάρχει κίνδυνος εισαγωγής κακόβουλου λογισμικού κατά την επίσκεψη τους σε διαδικτυακές ιστοσελίδες. Εάν κάποιος χρήστης ανακαλύψει ότι επισκέφθηκε κάποιο ιστότοπο που φαίνεται να ενεργεί ασυνήθιστα, θα πρέπει να αποσυνδεθεί αμέσως από αυτόν και να αναφέρει το συμβάν στην Διεύθυνση Ψηφιακής Διακυβέρνησης.

Κατά την πλοήγησή τους στο διαδίκτυο, οι χρήστες πρέπει να:

- *χρησιμοποιούν πάντα την τελευταία έκδοση του web browser[7] και να τον ρυθμίσουν ώστε να λαμβάνει ενημερώσεις αυτόματα*
- *απενεργοποιήσουν τα περιττά browser plugins και extensions[8]*
- *μην επιλέγουν την αποθήκευση των κωδικών πρόσβασης στον web browser*
- *πλοηγούνται στο Διαδίκτυο με ασφάλεια, αποφεύγοντας ιστοσελίδες που είναι πιθανό να είναι μολυσμένες, όπως ιστοσελίδες παράνομου διαμοιρασμού ταινιών, μουσικής, λογισμικού κ.λπ.*
- *επιβεβαιώνουν ότι κάθε ιστοσελίδα μέσω της οποίας αποστέλλουν προσωπικές πληροφορίες (κωδικούς πρόσβασης, αριθμό πιστωτικής κάρτας κ.α.) λειτουργεί με το πρωτόκολλο https. Αυτό σημαίνει ότι: α) η διεύθυνση αρχίζει με "https://" και β) αριστερά του "https://" υπάρχει ένα μικρό λουκέτο, που δηλώνει ότι η σύνδεση είναι ασφαλής και ότι η ιστοσελίδα διαθέτει ισχύον πιστοποιητικό (valid certificate)*
- *δίνουν ιδιαίτερη προσοχή στο είδος των πληροφοριών της προσωπικής και επαγγελματικής τους ζωής που αναρτούν στα κοινωνικά δίκτυα.*

6.3 Απαγόρευση πρόσβασης σε ιστοτόπους από την ΕΕΤΤ

Η ΕΕΤΤ διατηρεί το δικαίωμα απαγόρευσης της πρόσβασης σε συγκεκριμένες διαδικτυακές σελίδες (π.χ. ιστοσελίδες σχετικές με ενήλικο/σεξουαλικό περιεχόμενο, εγκληματικές ενέργειες, τυχερά παιχνίδια, ναρκωτικά, αλκοόλ, ρητορική μίσους, βία, όπλα κτλ.) σύμφωνα με την ισχύουσα νομοθεσία. Ως εκ τούτου, η πρόσβαση σε τέτοιους ιστοτόπους απαγορεύεται.

Εάν οι χρήστες, κατά την περιήγησή τους στο Διαδίκτυο, επισκεφθούν έναν ιστότοπο που δεν συμμορφώνεται με τις γενικές αρχές της παρούσας πολιτικής, θα πρέπει να αποσυνδεθούν αμέσως.

Να σημειωθεί ότι ενδεχόμενη δυνατότητα ενός χρήστη να επισκεφθεί μία ακατάλληλη και παράνομη ιστοσελίδα, δεν σημαίνει ότι η πρόσβασή του σε αυτή είναι αποδεκτή από την ΕΕΤΤ.

[7] *Web browser είναι μια εφαρμογή που παρέχει πρόσβαση σε ιστοτόπους.*

[8] *Browser plugins και extensions είναι μικρά λογισμικά προσαρμογής του web browser ως προς την διεπαφή χρήστη, την διαχείριση cookies, τον αποκλεισμό διαφημίσεων και του στυλ των ιστοσελίδων. Η κύρια διαφορά είναι ότι τα browser extensions διανέμονται ως πηγαίος κώδικας, ενώ τα browser plugins διανέμονται ως εκτελέσιμα.*

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

6.4 Μέσα κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης επιτρέπουν την δημιουργία και ανταλλαγή περιεχομένου που παράγεται από τους χρήστες σχετικά με προσωπικές πληροφορίες και απόψεις. Μέσα κοινωνικής δικτύωσης θεωρούνται τα blogs, τα φόρουμ ειδικού ενδιαφέροντος, οι ιστότοποι κοινωνικής δικτύωσης (π.χ. Facebook, Twitter, LinkedIn, Instagram) κτλ. Σε περιπτώσεις που πραγματοποιείται χρήση των μέσων κοινωνικής δικτύωσης, ισχύουν τα εξής:

- *Η χρήση των μέσων κοινωνικής δικτύωσης πρέπει να συμμορφώνεται με τις σχετικές πολιτικές της ΕΕΤΤ.*
- *Όλες οι πληροφορίες σχετικά με την ΕΕΤΤ πρέπει να διαχειρίζονται σύμφωνα με την πολιτική απορρήτου της ΕΕΤΤ. Μόνο εξουσιοδοτημένα άτομα επιτρέπεται να δημοσιεύουν και να κοινοποιούν πληροφορίες σχετικά με την ΕΕΤΤ.*
- *Οι κωδικοί πρόσβασης που χρησιμοποιούνται στους λογαριασμούς μέσων κοινωνικής δικτύωσης δεν πρέπει να είναι ίδιοι με αυτούς που χρησιμοποιούνται για υπηρεσιακούς σκοπούς.*
- *Οι χρήστες που έχουν πρόσβαση σε μέσα κοινωνικής δικτύωσης πρέπει να βεβαιωθούν ότι οι συσκευές που χρησιμοποιούν έχουν τις κατάλληλες ρυθμίσεις και συντηρούνται σωστά.*
- *Οι διαδικτυακές δραστηριότητες των χρηστών μπορεί να παρακολουθούνται και να καταγράφονται, ώστε να διασφαλίζεται η προστασία των πόρων της ΕΕΤΤ από κακή χρήση και η αποφυγή απώλειας δεδομένων.*

Για διευκρινίσεις σχετικά με τα παραπάνω, πρέπει να ερωτάται η Διεύθυνση Ψηφιακής Διακυβέρνησης ή/και ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ/DPO).

6.5 Δημοσιοποίηση πληροφοριών της ΕΕΤΤ

Οι χρήστες πρέπει να είναι πολύ προσεκτικοί κατά την δημοσίευση πληροφοριών ή ερωτήσεων στο Διαδίκτυο (π.χ. μέσω λιστών αλληλογραφίας, φόρουμ κτλ.), προκειμένου να μη βλάψουν την δημόσια εικόνα της ΕΕΤΤ.

Δεν επιτρέπεται η δημοσίευση σε σελίδες του Διαδικτύου ή η αποστολή μέσω Διαδικτύου, εμπιστευτικών πληροφοριών της ΕΕΤΤ. Οι χρήστες πρέπει να γνωρίζουν ότι ένας κακόπιστος τρίτος μπορεί να συνδυάσει μία σειρά από φαινομενικά ασύνδετες πληροφορίες, προκειμένου να ανακαλύψει ευαίσθητες πληροφορίες της ΕΕΤΤ, οι οποίες μπορούν να χρησιμοποιηθούν εναντίον της.

6.6 Επικοινωνία με εξωτερικές οντότητες

Οι χρήστες που επιθυμούν να επικοινωνήσουν με τρίτες οντότητες (προμηθευτές, παρόχους κτλ.) για υπηρεσιακούς σκοπούς πρέπει να χρησιμοποιούν αποκλειστικά το σύστημα ηλεκτρονικού ταχυδρομείου της ΕΕΤΤ και την εκχωρημένη σε αυτούς διεύθυνση ηλεκτρονικού ταχυδρομείου.

Οι χρήστες δεν πρέπει να αποστέλλουν, λαμβάνουν ή διαβιβάζουν υπηρεσιακές πληροφορίες με χρήση διευθύνσεων ηλεκτρονικού ταχυδρομείου εκτός ΕΕΤΤ, όπως το Gmail, Hotmail, Yahoo κτλ. Ακόμα και σε περιπτώσεις όπου οι εργαζόμενοι πρέπει να αποστείλουν ένα υπηρεσιακό μήνυμα ενώ βρίσκονται απομακρυσμένα δεν πρέπει να χρησιμοποιούν άλλα συστήματα ηλεκτρονικού ταχυδρομείου, εκτός εάν κάτι τέτοιο έχει εγκριθεί ρητά.

Αντιθέτως, πρέπει να αποφεύγεται η αποστολή μη υπηρεσιακών δεδομένων και αρχείων μέσω του υπηρεσιακού ηλεκτρονικού ταχυδρομείου.

Ο λογαριασμός ηλεκτρονικού ταχυδρομείου του κάθε χρήστη είναι ατομικός και δεν πρέπει να μοιράζεται σε άλλους. Δεν επιτρέπεται η χρήση του για την αποστολή ή λήψη υλικού πνευματικής ιδιοκτησίας τρίτων παραβιάζοντας τα δικαιώματα περί πνευματικής ιδιοκτησίας. Δεν επιτρέπεται η αλλοίωση οποιασδήποτε πληροφορίας σχετικά με την προέλευση ενός μηνύματος (αποστολέα, αποδέκτη, ημερομηνίας και ώρας αποστολής κτλ.).

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

6.7 Διακίνηση προσβλητικών μηνυμάτων και δημοσιεύσεων

Απαγορεύεται ρητά η διακίνηση μηνυμάτων με παράνομο ή άσεμνο περιεχόμενο και μηνυμάτων με κακόβουλο λογισμικό. Επίσης, απαγορεύεται ρητά η αποστολή σε άλλους χρήστες ανεπιθύμητων μηνυμάτων και διαφημιστικού ή προωθητικού περιεχομένου.

Ειδικότερα, οι χρήστες δεν πρέπει να αποστέλλουν ή να προωθούν μηνύματα άμεσα/μηνύματα ηλεκτρονικού ταχυδρομείου ή δημοσιεύσεις που προσβάλουν, συκοφαντούν, δυσφημούν, απειλούν, ενοχλούν ή κακοποιούν με οποιονδήποτε τρόπο άτομα, νομικά πρόσωπα, χώρες, έθνη, εθνικότητες, σεξουαλικούς προσανατολισμούς, θρησκείες, πολιτικές πεποιθήσεις και σωματικές αναπηρίες, καθώς και μηνύματα που ενδέχεται να έχουν νομικές ή άλλες συνέπειες για την δημόσια εικόνα της ΕΕΤΤ.

Οι χρήστες δεν πρέπει να χρησιμοποιούν χυδαία, καταχρηστική ή οποιουδήποτε άλλου είδους ακατάλληλη γλώσσα σε μηνύματα που απευθύνονται σε συναδέλφους, παρόχους, δημόσιους φορείς ή τρίτα πρόσωπα.

Επιπλέον, απαγορεύεται αυστηρά η αποστολή, προώθηση και αποθήκευση πληροφοριών και αρχείων που σχετίζονται με παράνομες ή ανάρμοστες δραστηριότητες (π.χ. πορνεία, εμπορία ναρκωτικών, τρομοκρατία, άλλες εγκληματικές ενέργειες κτλ.).

Η ΕΕΤΤ φέρει την ευθύνη για τον ορισμό αυτού που συνιστά ένα προσβλητικό μήνυμα /δημοσίευση ή ένα μήνυμα/δημοσίευση με προσβλητικό περιεχόμενο, όπως τα ανωτέρω παραδείγματα.

Οι χρήστες θα υπόκεινται σε πειθαρχικές κυρώσεις σε περίπτωση σκόπιμης παραβίασης των παραπάνω.

6.8 Εκπροσώπηση της ΕΕΤΤ στο Διαδίκτυο

Ένα μήνυμα από το υπηρεσιακό ηλεκτρονικό ταχυδρομείο που αποστέλλεται από έναν υπάλληλο σε έναν πάροχο, προμηθευτή, δημόσια υπηρεσία και γενικά σε τρίτη οντότητα, εκλαμβάνεται από αυτή την τρίτη οντότητα ως μήνυμα με αποστολέα την ΕΕΤΤ. Επομένως, απαγορεύεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου με προσωπικές απόψεις για προσωπική χρήση μέσω του υπηρεσιακού λογαριασμού e-mail της ΕΕΤΤ.

Η χρήση του υπηρεσιακού λογαριασμού e-mail πρέπει να συμμορφώνεται με την παρούσα πολιτική και οι χρήστες να ενεργούν κατά τρόπο που ενισχύει την εικόνα της ΕΕΤΤ και δεν βλάπτει τα συμφέροντά της με οποιονδήποτε τρόπο.

Επίσης, οι χρήστες δεν πρέπει να συνάπτουν συμφωνίες ή να πραγματοποιούν διαπραγματεύσεις μέσω του Διαδικτύου που μπορούν να δεσμεύσουν την ΕΕΤΤ με οποιονδήποτε τρόπο, εκτός εάν υπάρχει ρητή εξουσιοδότηση για κάτι τέτοιο.

6.9 Ασφαλής μετάδοση της πληροφορίας

Οι χρήστες πρέπει να γνωρίζουν ότι οι πληροφορίες που διακινούνται μέσω ηλεκτρονικού ταχυδρομείου ή του Διαδικτύου μπορούν να προωθούνται, να παρεμποδίζονται, να εκτυπώνονται και να αποθηκεύονται από μη εξουσιοδοτημένους χρήστες, εκτός εάν χρησιμοποιούνται επαρκείς τεχνολογίες ασφάλειας οι οποίες μπορούν να διασφαλίσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους (π.χ. κρυπτογράφηση, ηλεκτρονικές υπογραφές κτλ.). Επομένως, οι χρήστες δεν πρέπει να διακινούν εμπιστευτικές ή απόρρητες πληροφορίες και προσωπικά δεδομένα μέσω του ηλεκτρονικού ταχυδρομείου ή του Διαδικτύου χωρίς τη λήψη μέτρων που καθιστούν ασφαλή τη μετάδοση της πληροφορίας.

6.10 Χρήση της αποποίησης ευθυνών (disclaimer)

Η εμπιστευτικότητα των πληροφοριών που αποστέλλονται μέσω ηλεκτρονικού ταχυδρομείου πρέπει να διασφαλίζεται ακόμα και σε περίπτωση λανθασμένης παράδοσης.

Για τον σκοπό αυτό, κάθε εμπιστευτικό μήνυμα που αποστέλλεται από διεύθυνση ηλεκτρονικού ταχυδρομείου της ΕΕΤΤ πρέπει να περιέχει την κατάλληλη αποποίηση ευθυνών (disclaimer) αναφορικά με την εμπιστευτικότητα.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

6.11 Αποστολή μαζικών μηνυμάτων (bulk messages)

Προκειμένου να αποφευχθεί η υπερφόρτωση του δικτύου και των συστημάτων, πρέπει να αποφεύγεται η αποστολή μηνυμάτων με χρήση λιστών διανομής (distribution list) και ομαδικών λιστών (group lists), εντός και εκτός της ΕΕΤΤ, εκτός εάν υπάρχει υπηρεσιακή ανάγκη για κάτι τέτοιο.

Επιπλέον, για την αποστολή μαζικών μηνυμάτων ηλεκτρονικού ταχυδρομείου εκτός της ΕΕΤΤ, απαιτείται ρητή εξουσιοδότηση.

6.12 Χειρισμός κατά τη λήψη κακόβουλων / προσβλητικών μηνυμάτων

Οι χρήστες δεν πρέπει να απαντούν απευθείας στον αποστολέα κακόβουλων / προσβλητικών μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου ή άλλης υπηρεσίας ανταλλαγής μηνυμάτων.

Εάν ο αποστολέας αποστέλλει επανειλημμένα προσβλητικά μηνύματα, οι χρήστες πρέπει να το αναφέρουν άμεσα στην Διεύθυνση Ψηφιακής Διακυβέρνησης.

Ιδιαίτερη προσοχή πρέπει να δοθεί στην αποφυγή της διαγραφής μηνυμάτων ή δεδομένων που συνεπάγεται την καταστροφή αποδεικτικών στοιχείων που θα βοηθούσαν σε εσωτερικές πειθαρχικές ή εξωτερικές νομικές διαδικασίες.

6.13 Προσεκτική χρήση συνημμένων και υπερσυνδέσμων

Οι χρήστες δεν πρέπει ποτέ να ανοίγουν αρχεία που επισυνάπτονται σε μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία προέρχονται από άγνωστα, ύποπτα ή μη αξιόπιστα πρόσωπα.

Οι χρήστες δεν πρέπει να ακολουθούν υπερσυνδέσμους οι οποίοι βρίσκονται σε μηνύματα ή e-mail και τα οποία προέρχονται από άτομα των οποίων η αξιοπιστία δεν έχει επιβεβαιωθεί.

Οι χρήστες πρέπει να αναφέρουν τέτοιου είδους περιστατικά (π.χ. ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου) στην Διεύθυνση Ψηφιακής Διακυβέρνησης και να συμμορφώνονται με τις οδηγίες της.

6.14 Αντιμετώπιση επιθέσεων ηλεκτρονικού ψαρέματος (phishing)

Οι χρήστες πρέπει να είναι προσεκτικοί ώστε να αναγνωρίζουν και να αγνοούν μηνύματα ηλεκτρονικού ταχυδρομείου ή/και άμεσα μηνύματα που τους παροτρύνουν να επισκέπτονται ιστοτόπους και να αποκαλύπτουν εμπιστευτικές πληροφορίες ή προσωπικά δεδομένα, όπως ονόματα χρηστών και κωδικούς πρόσβασης. Αναφορικά με τέτοια μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται από συνεργάτες ή τρίτους, οι χρήστες πρέπει να αναφέρουν αμέσως το συμβάν στην Διεύθυνση Ψηφιακής Διακυβέρνησης.

Τέτοια κακόβουλα μηνύματα συνήθως διαθέτουν μερικά κοινά χαρακτηριστικά τα οποία μπορούν να βοηθήσουν στην αναγνώρισή τους. Ενδεικτικά:

- *είναι αυτόκλητα*
- *συνήθως αποτελούν παραλλαγή γνήσιων μηνυμάτων*
- *συχνά μιμούνται/χρησιμοποιούν κρατικές υπηρεσίες ή μεγάλες επιχειρήσεις με τις οποίες υπάρχει πιθανότητα να συνεργάζεται ο παραλήπτης αλλά διαφέρουν σημαντικά από άλλα μηνύματα που έχουν ληφθεί από αυτή την κρατική υπηρεσία ή μεγάλη επιχείρηση*
- *σε γενικές γραμμές είναι μη επαγγελματικά ή ερασιτεχνικά συνταγμένα*
- *παρουσιάζουν προβλήματα στην επωνυμία (λογότυπο και φόντο εικόνας) ή στην κεφαλίδα τους*
- *σε ορισμένες περιπτώσεις έχουν εμφανή λάθη στην χρήση της ελληνικής γλώσσας, όπως ορθογραφικά, συντακτικά, γραμματικά λάθη*
- *συχνά κάνουν περίεργη χρήση των κεφαλαίων γραμμάτων, π.χ. κάποιες τυχαίες λέξεις μέσα στο κείμενο είναι γραμμένες με κεφαλαία ή αντίθετα έχουν μικρό γράμμα στην αρχή πρότασης*
- *μέρος του κειμένου μπορεί να είναι σε ξένη γλώσσα διαφορετική από την γλώσσα αποστολής*
- *η υπογραφή δεν είναι ολοκληρωμένη*

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

- *ζητούν προσωπικές πληροφορίες μέσω email που κανένας οργανισμός ή εταιρεία δεν θα ζητούσε, όπως όνομα χρήστη, κωδικούς, πληροφορίες τραπεζικών λογαριασμών κτλ.*
- *ενώ το μήνυμα φαίνεται να αποστέλλεται από κρατική υπηρεσία ή ιδιωτική επιχείρηση (πχ. από @aade.gr ή @gov.gr), ο πραγματικός αποστολέας είναι άγνωστη ηλεκτρονική διεύθυνση, συνήθως στην αλλοδαπή, που δεν αντιστοιχεί στην υπηρεσία ή επιχείρηση από την οποία υποτίθεται ότι προέρχεται*
- *η διεύθυνση απάντησης είναι διαφορετική από του αποστολέα και δεν έχει σχέση με την υπηρεσία ή επιχείρηση από την οποία υποτίθεται ότι προέρχεται*
- *προτρέπουν τον παραλήπτη να επιλέξει/επισκεφτεί κάποιο σύνδεσμο που φαίνεται σωστός, αλλά η διεύθυνση URL δεν αντιστοιχεί στην υπηρεσία ή επιχείρηση από την οποία υποτίθεται ότι προέρχεται το μήνυμα*
- *συχνά υπάρχει ένας επείγων χαρακτήρας στον ζητούμενο χρόνο απόκρισης, που πιέζει τον παραλήπτη να λάβει μια βιαστική απόφαση και δεν του αφήνει χρόνο να αμφισβητήσει την γνησιότητα του μηνύματος*
- *τέτοια πλαστά μηνύματα ορισμένες φορές δημιουργούν μία ατμόσφαιρα συνομωσίας*
- *συχνά ισχυρίζονται ότι υπάρχει ύποπτη δραστηριότητα στον λογαριασμό ή την συσκευή του παραλήπτη ή προβλήματα ασφάλειας, για να τραβήξουν την προσοχή*
- *το περιεχόμενό τους δεν είναι κατανοητό ή προκαλεί εύλογες απορίες, γιατί, για παράδειγμα, δεν έχει σχέση με τις αρμοδιότητες της ΕΕΤΤ*
- *τα παραπλανητικά μηνύματα ενδέχεται να χρησιμοποιούν κολακείες ή απειλές προκειμένου να πιέσουν τον παραλήπτη να παρέχει πληροφορίες*
- *συχνά υπόσχονται μεγάλα οφέλη, όπως κάποιο χρηματικό ποσό, δωρεάν προϊόντα και έπαθλα, εάν ο παραλήπτης παρέχει τις ζητούμενες πληροφορίες ή τα προωθήσει σε όλες τις επαφές του ή απειλούν ότι θα του συμβούν άσχημα πράγματα σε αντίθετη περίπτωση.*

Στην περίπτωση που λάβουν εισερχόμενο email που φαίνεται ύποπτο, οι χρήστες πρέπει να:

- *είναι ιδιαιτέρως επιφυλακτικοί, να ελέγξουν ορθολογικά και να διερευνήσουν τις πληροφορίες που παρέχει το μήνυμα*
- *επαληθεύσουν την ταυτότητα του αποστολέα (π.χ. μέσω τηλεφώνου)*
- *μην ανοίξουν μήνυμα που φαίνεται να αφορά κάποια επείγουσα κατάσταση ή έκτακτη ανάγκη ή περιέχει περίεργους ισχυρισμούς και προσφορές που είναι πολύ καλές για να είναι αληθινές*
- *μην ανοίξουν κανένα συνημμένο αρχείο του μηνύματος, καθώς μπορεί να περιέχει κακόβουλο λογισμικό που θα μολύνει τον υπολογιστή*
- *για τα μηνύματα που περιέχουν συνδέσμους, να αναζητήσουν την ιστοσελίδα μέσω μίας μηχανής αναζήτησης*
- *μην επιλέξουν/επισκεφθούν το σύνδεσμο που τυχόν υπάρχει στο κείμενο του μηνύματος, διότι ο σύνδεσμος μπορεί να είναι μία ψεύτικη ιστοσελίδα που θα ζητά τους κωδικούς ή άλλες πληροφορίες του χρήστη. Κανένας οργανισμός (όπως τράπεζες, Δημόσιες Αρχές κ.α.) δεν πρόκειται ποτέ να ζητήσει μέσω email τέτοια στοιχεία*
- *μην απαντούν στα ύποπτα μηνύματα, μην παρέχουν ιδιωτικές ή εμπιστευτικές πληροφορίες και μην εισάγουν κωδικούς πρόσβασης*
- *να διαγράψουν αμέσως το μήνυμα εφόσον οι παραπάνω επαληθεύσεις αποτύχουν*
- *να αναφέρουν το συμβάν στη Διεύθυνση Ψηφιακής Διακυβέρνησης.*

6.15 Πλαστογράφηση ταυτότητας χρηστών

Η πλαστογράφηση ή η απόπειρα πλαστογράφησης της ταυτότητας χρήστη (ταυτότητα αποστολέα) μέσω υπηρεσιών ηλεκτρονικού ταχυδρομείου και Διαδικτύου απαγορεύεται αυστηρά. Το όνομα χρήστη, η διεύθυνση

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

ηλεκτρονικού ταχυδρομείου, ο ρόλος του μέσα στην ΕΕΤΤ και άλλες σχετικές πληροφορίες που περιέχονται σε μηνύματα ηλεκτρονικού ταχυδρομείου και αναρτήσεις πρέπει να προσδιορίζουν τον πραγματικό αποστολέα.

6.16 Πρόσβαση σε κοινόχρηστους λογαριασμούς ηλεκτρονικού ταχυδρομείου

Η πρόσβαση στους κοινόχρηστους λογαριασμούς ηλεκτρονικού ταχυδρομείου της ΕΕΤΤ, πρέπει να περιορίζεται αποκλειστικά στους χρήστες που είναι επιφορτισμένοι με την αποστολή και λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου από τους λογαριασμούς αυτούς, καθώς και με την ανάληψη δράσης σε σχέση με τα μηνύματα αυτά.

Η πρόσβαση μη εξουσιοδοτημένων χρηστών σε κοινόχρηστους λογαριασμούς ηλεκτρονικού ταχυδρομείου απαγορεύεται αυστηρά.

6.17 Εγγραφή σε μη εγκεκριμένες υπηρεσίες και λίστες αλληλογραφίας

Η εγγραφή των χρηστών σε υπηρεσίες που δεν έχουν εγκριθεί από την ΕΕΤΤ, όπως λίστες αλληλογραφίας, μέσα κοινωνικής δικτύωσης κτλ. με χρήση των λογαριασμών ηλεκτρονικού ταχυδρομείου της ΕΕΤΤ για προσωπική χρήση απαγορεύεται αυστηρά.

6.18 Ανάκληση πρόσβασης στο Διαδίκτυο και στο ηλεκτρονικό ταχυδρομείο

Η ΕΕΤΤ διατηρεί το δικαίωμα ανάκλησης της πρόσβασης των χρηστών στο Διαδίκτυο και το ηλεκτρονικό ταχυδρομείο σε περίπτωση ακατάλληλης χρήσης εκ μέρους τους, δηλαδή χρήσης που δεν συμμορφώνεται με την παρούσα πολιτική.

7 Καθαρή επιφάνεια εργασίας και οθόνη

7.1 Ψηφιακά υπηρεσιακά δεδομένα και έντυπα

Οι χρήστες πρέπει να λαμβάνουν μέριμνα για την όσο το δυνατόν καθαρή επιφάνεια εργασίας. Δεν πρέπει να αφήνουν εκτεθειμένα, χωρίς επίβλεψη ευαίσθητα ή κρίσιμα υπηρεσιακά έγγραφα που είναι σε έντυπη μορφή (π.χ. εκτυπώσεις) στα γραφεία τους ή στην ευρύτερη περιοχή εργασίας τους.

Όταν εκτυπώνουν ευαίσθητη πληροφόρηση πρέπει να διασφαλίζουν ότι η εκτύπωση παραμένει ασφαλής, δηλαδή να επιβεβαιώνουν την τοποθεσία του εκτυπωτή που έστειλαν την εκτύπωση, να αφαιρούν άμεσα από τον εκτυπωτή την εκτύπωση, να καταστρέφουν με ασφαλή τρόπο όσες εκτυπώσεις δεν χρειάζονται.

Όλα αυτά τα έγγραφα πρέπει να κλειδώνονται με ασφάλεια στα γραφεία, αρχειοθήκες ή σε καθορισμένους ασφαλείς χώρους, ανά πάσα στιγμή, πέραν αυτής κατά την οποία γίνεται η χρήση τους.

Με την ευκαιρία, επισημαίνεται, επίσης, ότι είναι ευθύνη των χρηστών να διασφαλίζουν την λήψη όλων των απαραίτητων προφυλάξεων ασφάλειας σε σχέση με τα προσωπικά τους αντικείμενα, όπως προσωπικά αρχεία, κλειδιά, κάρτες πρόσβασης κτλ.

7.2 Κλείδωμα υπολογιστών, φορητών υπολογιστών, τερματικών όταν δεν υπάρχει επιτήρηση

Οι υπολογιστές, οι φορητοί υπολογιστές, τα smartphones ή/και οι τερματικοί σταθμοί δεν πρέπει να παραμένουν συνδεδεμένοι εκτός και εάν επιτηρούνται από τους χρήστες τους.

Εάν οι χρήστες πρέπει να εγκαταλείψουν τα γραφεία τους για οποιονδήποτε λόγο, πρέπει να κλειδώσουν τον υπολογιστή χρησιμοποιώντας τα πλήκτρα «Control, Alt, Del» ταυτόχρονα (ή οποιοδήποτε κατάλληλο συνδυασμό).

Επίσης, οι χρήστες πρέπει να κλείνουν τα συστήματά τους πριν εγκαταλείψουν το γραφείο τους στο τέλος της εργασιακής ημέρας.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

8 Ορθή χρήση τηλεφωνικού εξοπλισμού και υπηρεσιών

8.1 Χρήση τηλεφωνικού εξοπλισμού

Στους χρήστες ενδέχεται να ανατεθεί η χρήση τηλεφωνικού εξοπλισμού της ΕΕΤΤ ως μέσο διευκόλυνσης της εκτέλεσης των υπηρεσιακών τους καθηκόντων, όπως η επικοινωνία με την Διοίκηση, συναδέλφους, συνεργάτες, παρόχους, η επικοινωνία στις επιφυλακές κτλ.

Ο τηλεφωνικός εξοπλισμός θεωρείται περιουσιακό στοιχείο της ΕΕΤΤ και ως εκ τούτου η χρήση του πρέπει να συμμορφώνεται με την παρούσα πολιτική και να μην χρησιμοποιείται για προσωπικούς σκοπούς, εκτός εάν κάτι τέτοιο έχει επιτραπεί.

Οι χρήστες πρέπει να επιδεικνύουν την δέουσα προσοχή όταν πραγματοποιούν υπεραστικές ή/και διεθνείς κλήσεις, ενώ θα πρέπει να αναζητούνται και εναλλακτικές μέθοδοι επικοινωνίας (π.χ. εξουσιοδοτημένο λογισμικό διαδικτυακής διάσκεψης).

Οι χρήστες πρέπει να διασφαλίζουν πάντα ότι γνωρίζουν ποιος τους ζητά στοιχεία και ότι είναι εξουσιοδοτημένος να έχει πρόσβαση στην πληροφορία που ζητά. Δεν πρέπει να απαντούν σε ερωτήματα σχετικά με προσωπικά δεδομένα άλλων υπαλλήλων της ΕΕΤΤ. Δεν πρέπει να δίνουν στοιχεία αυθεντικοποίησης μέσω τηλεφώνου σε τρίτους. Δεν πρέπει να δίνουν ευαίσθητη πληροφόρηση της ΕΕΤΤ μέσω τηλεφώνου σε τρίτους.

8.2 Μη εξουσιοδοτημένη ή/και προσβλητική χρήση της υπηρεσίας τηλεφωνίας

Οι χρήστες δεν πρέπει να χρησιμοποιούν την υπηρεσία τηλεφωνίας:

- *για καταχρηστικές, βίαιες, συκοφαντικές, απειλητικές ή παρενοχλητικές κλήσεις*
- *για να συστήσουν ή να λάβουν μέρος σε παράνομες δραστηριότητες, όπως οικονομικές απάτες, καθώς και για κλοπή ταυτότητας και πληροφοριών*
- *για τη μετάδοση οποιουδήποτε υλικού το οποίο παραβιάζει οποιοδήποτε δικαίωμα πνευματικής ιδιοκτησίας, εμπορικού σήματος, διπλώματος ευρεσιτεχνίας, εμπορικού μυστικού ή άλλων δικαιωμάτων ιδιοκτησίας τρίτου μέρους*
- *για την συλλογή ή προσπάθεια συλλογής προσωπικών πληροφοριών σχετικά με τρίτους χωρίς τη γνώση ή την συγκατάθεσή τους*
- *για αυτόματη κλήση, συνεχή ή εκτεταμένη προώθηση κλήσεων, τηλεφωνικές πωλήσεις (συμπεριλαμβανομένων φιλανθρωπικών και πολιτικών προσκλήσεων και ψηφοφοριών) κτλ., εάν δεν υπάρχει προηγούμενη έγκριση.*

8.3 Ορθή χρήση Internet Protocol (IP) τηλεφωνίας

Οι τεχνολογικές εξελίξεις διευκολύνουν την χρήση IP τηλεφωνίας έναντι της παραδοσιακής τηλεφωνικής υπηρεσίας και του εξοπλισμού που την συνοδεύει και υποδηλώνουν ότι η χρήση της τεχνολογίας αυτής, με οποιονδήποτε τρόπο, πρέπει να συμμορφώνεται με την παρούσα πολιτική.

Οποιαδήποτε προσπάθεια παραβίασης της ασφάλειας τέτοιου είδους εξοπλισμού απαγορεύεται. Οι χρήστες δεν πρέπει να εκτελούν κανένα πρόγραμμα παρακολούθησης πακέτων δεδομένων στο δίκτυο ή οποιοδήποτε άλλο πρόγραμμα που θέτει σε κίνδυνο την ιδιωτικότητα της κίνησης στο δίκτυο.

Οι παρεμβολές στην υπηρεσία, συμπεριλαμβανομένων των εσκεμμένων προσπαθειών υπερφόρτωσης του συστήματος, απαγορεύονται αυστηρά.

Οι χρήστες δεν πρέπει να χρησιμοποιούν την υπηρεσία προκειμένου να παρακολουθούν άλλους χρήστες, να θέτουν σε κίνδυνο την ακεραιότητα των κλήσεων ή/και να εκτελούν επιθέσεις άρνησης εξυπηρέτησης

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr

υπηρεσιών (Denial of Service - DoS)[9], που καθιστούν το σύστημα μη προσβάσιμο στους προοριζόμενους χρήστες του.

»

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

Γ. **Ορίζει** ότι η «Πολιτική Ασφάλειας Τελικού Χρήστη» συνδέεται άρρηκτα με την υπό στοιχείο 7. ως άνω «Πολιτική Ασφαλείας της ΕΕΤΤ» και την υπό στοιχείο 8. ως άνω «Πολιτική Αποδεκτής Χρήσης των Πληροφοριακών Αγαθών της ΕΕΤΤ» και πρέπει να εφαρμόζεται υποχρεωτικά και απαρέγκλιτα από τους χρήστες των συστημάτων πληροφορικής και επικοινωνιών της ΕΕΤΤ. Οποιαδήποτε εξαίρεση από την παρούσα Πολιτική θα εγκρίνεται με απόφαση Προέδρου, πριν από οποιαδήποτε ενέργεια.

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 Ασφάλειας Τελικού Χρήστη».
- Τροποποιεί την «Πολιτική Ασφάλειας Τελικού Χρήστη» σε τακτική βάση σύμφωνα με τις ανάγκες της ΕΕΤΤ, προκειμένου να προσαρμόζεται στις εκάστοτε καταστάσεις, κινδύνους και περιορισμούς.

Ο ΠΡΟΕΔΡΟΣ

ΚΑΘΗΓΗΤΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ ΜΑΣΣΕΛΟΣ

[9] Επιθέσεις άρνησης εξυπηρέτησης (DoS attack) ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες.

Ελληνική Δημοκρατία - Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Λεωφ. Κηφισίας 60
151 25 Μαρούσι
Τηλ.: 210 615 1000
Fax: 210 610 5049
www.eett.gr