ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

Μαρούσι, 10-06-2024

ΑΠ: 1115/11

ΑΠΟΦΑΣΗ

Έγκριση της «Πολιτικής Διαχείρισης Πληροφοριακών Πόρων»

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ),

Έχοντας υπόψη:

1. Τις διατάξεις:

1.1 του Ν. 4070/2012 «*Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις*» (ΦΕΚ 82/Α/2012), όπως ισχύει τροποποιηθείς,

1.2 του Ν. 4053/2012 *«Ρύθμιση λειτουργίας της ταχυδρομικής αγοράς, θεμάτων ηλεκτρονικών επικοινωνιών και άλλες διατάξεις»* (ΦΕΚ 44/Α/2012), όπως ισχύει τροποποιηθείς,

1.3 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),

1.4 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),

1.5 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),

1.6 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*

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

επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις», (ΦΕΚ 199/ Α' /03-12-2018), όπως ισχύει,

1.7 του Ν. 4961/2022 «*Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις*», (ΦΕΚ 146/Α'/27-7-2022),

1.8 του Ν. 5002/2022 «*Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών*», (ΦΕΚ 228/Α΄/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 εγκεκριμένη από τον Πρόεδρο της ΕΕΤΤ «*Πολιτική Ασφαλείας της ΕΕΤΤ, έκδοση 1.0*» με αριθ. πρωτ. 278/1-6-2018,

5. Την ΑΠ 989/25/26-04-2021 Απόφαση της ΕΕΤΤ «*Έγκριση της εφαρμογής της αναθεωρημένης "Πολιτικής Αποδεκτής Χρήσης των Πληροφοριακών Αγαθών της ΕΕΤΤ*"»,

6. Την ΑΠ 1048/13/24-10-2022 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών"*»,

7. Την ΑΠ 1069/13/27-03-2023 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Ασφάλειας Τελικού Χρήστη"*»,

8. Την ΑΠ 1089/32/30-10-2023 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διατήρησης Πληροφοριών"*»,

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 1109/13/15-4-2024 Απόφαση της ΕΕΤΤ «*Επικύρωση του Εγχειριδίου Διαδικασιών της ΕΕΤΤ*»,
10. Την Εισήγηση αριθ. 37643/05-06-2024 της αρμόδιας Υπηρεσίας της ΕΕΤΤ,

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

Επειδή :

1. Η ΕΕΤΤ χρησιμοποιεί ευρέως πληροφοριακούς πόρους που είναι κρίσιμοι για την καθημερινή λειτουργία της, όπως πληροφορίες, πληροφοριακά συστήματα, λογισμικό και εξοπλισμό που επεξεργάζεται ή αποθηκεύει δεδομένα.
2. Κρίνεται σκόπιμη η υιοθέτηση μιας πολιτικής η οποία θα καθορίζει αρχές, κανόνες και μεθόδους για την επίτευξη και διατήρηση του κατάλληλου επιπέδου προστασίας και την πλήρη αξιοποίηση των πληροφοριακών πόρων της ΕΕΤΤ. Ειδικότερα, η πολιτική αυτή θα ρυθμίζει θέματα όπως η κατάρτιση μητρώου πληροφοριακών πόρων, ο καθορισμός του υπηρεσιακού ιδιοκτήτη και η εξουσιοδότηση χρήσης του κάθε πόρου, η ταξινόμηση / διαβάθμιση των πληροφοριακών πόρων ανάλογα με την κρισιμότητά τους και γενικότερα η ασφαλής διαχείρισή τους.

Αποφασίζει :

1. **Εγκρίνει** την «*Πολιτική Διαχείρισης Πληροφοριακών Πόρων*», η οποία ορίζει το σύνολο των αρχών, κανόνων και μεθόδων για την ασφαλή διαχείριση των πληροφοριακών πόρων της ΕΕΤΤ, στους οποίους συμπεριλαμβάνονται οι πληροφορίες και τα πληροφοριακά συστήματα, το λογισμικό και ο εξοπλισμός πληροφορικής. Η «*Πολιτική Διαχείρισης Πληροφοριακών Πόρων*» της ΕΕΤΤ έχει ως εξής:

« ***Πολιτική Διαχείρισης Πληροφοριακών Πόρων***

Έκδοση: 1η :

Ενημέρωση: Μάιος 2024

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

1. Σκοπός και πεδίο εφαρμογής

Σκοπός αυτής της πολιτικής είναι να ορίσει το σύνολο των αρχών, κανόνων και μεθόδων για την επίτευξη και διατήρηση του κατάλληλου επιπέδου προστασίας και την πλήρη αξιοποίηση των πληροφοριακών πόρων της ΕΕΤΤ.

Στον όρο πληροφοριακοί πόροι περιλαμβάνονται:

- *πληροφορίες και πληροφοριακά συστήματα (όπως ενδεικτικά βάσεις δεδομένων, ψηφιακά αρχεία, έγγραφα σε φυσική μορφή, αρχειοθετημένη πληροφορία, αρχεία καταγραφής (log files), κτλ.),*
- *λογισμικό (όπως εφαρμογές, λογισμικό συστημάτων και λειτουργικά συστήματα, λογισμικό ανάπτυξης εφαρμογών, άλλο βοηθητικό λογισμικό),*
- *εξοπλισμός (όπως ηλεκτρονικοί υπολογιστές, δικτυακός εξοπλισμός, μέσα αποθήκευσης και καταγραφής, εξοπλισμός διενέργειας ελέγχων/εποπτείας της ΕΕΤΤ και λοιπός τεχνικός εξοπλισμός που επεξεργάζεται ή αποθηκεύει δεδομένα).*

Η παρούσα πολιτική εφαρμόζεται από όλους, δηλαδή προσωπικό της ΕΕΤΤ, αναδόχους, συνεργάτες, τρίτους κτλ., των οποίων οι αρμοδιότητες σχετίζονται με την προμήθεια, ανάπτυξη, υλοποίηση, διαχείριση, χρήση, συντήρηση, απόσυρση των πληροφοριακών πόρων της ΕΕΤΤ.

Ο προσδοκώμενος στόχος της πολιτικής είναι οι πληροφοριακοί πόροι της ΕΕΤΤ να:

- *Είναι καταγεγραμμένοι.*
- *Έχουν καθορισμένο ιδιοκτήτη πληροφοριών με συγκεκριμένες ευθύνες.*
- *Έχουν ταξινομηθεί σύμφωνα με το σύστημα ταξινόμησης και τις σχετικές διαδικασίες της ΕΕΤΤ.*
- *Προστατεύονται κατάλληλα από ενδεχόμενες απειλές, σύμφωνα με το επίπεδο ταξινόμησής τους.*
- *Υφίστανται διαχείριση με ασφαλή τρόπο κατά την διάρκεια της ζωής τους (π.χ. να είναι κατάλληλα εγκατεστημένοι, λειτουργούντες, προσβάσιμοι, συντηρούμενοι, υποστηριζόμενοι κ.λ.π.).*

Ειδικότερα, η πολιτική καλύπτει τις ακόλουθες πτυχές ασφαλείας σχετικά με την διαχείριση πληροφοριακών πόρων, που αναλύονται παρακάτω:

- *Καθορισμός των Πληροφοριακών Πόρων.*
- *Καταγραφή Πληροφοριακών Πόρων.*
- *Καθεστώς Ιδιοκτησίας των Πληροφοριακών Πόρων.*
- *Ταξινόμηση Πληροφοριακών Πόρων.*
- *Εξουσιοδότηση για τη χρήση των Πληροφοριακών Πόρων.*
- *Γενικά Θέματα Διαχείρισης των Πληροφοριακών Πόρων.*

2. Προσδιορισμός και Καταγραφή των Πληροφοριακών Πόρων

2.1 Μητρώο Πληροφοριακών Πόρων

Προκειμένου η ΕΕΤΤ να αντιλαμβάνεται και να διαχειρίζεται τους πληροφοριακούς πόρους που κατέχει και τους κινδύνους που τους απειλούν, απαιτείται να προσδιορίζει και να καταγράφει οργανωμένα και συστηματικά τους πληροφοριακούς πόρους της.

Για το σκοπό αυτό, η ΕΕΤΤ τηρεί Μητρώο Πληροφοριακών Πόρων το οποίο περιλαμβάνει για κάθε πληροφοριακό πόρο, κατ' ελάχιστον, πληροφορίες που προσδιορίζουν τον πληροφοριακό πόρο, δεδομένα για την αποτίμηση της υπηρεσιακής αξίας του και στοιχεία για την εκτίμηση των κινδύνων που ενέχει. Ενδεικτικά, τέτοιες πληροφορίες που μπορούν να τηρούνται στο μητρώο, κατά περίπτωση, είναι ένας μοναδικός αναγνωριστικός κωδικός (που ενδεχομένως να συνδέεται με την κωδικοποίηση του Εγχειριδίου Διαδικασιών της ΕΕΤΤ), το όνομα του πληροφοριακού πόρου, η περιγραφή του, η τοποθεσία του, η σχετική διεργασία ή/και διαδικασία της ΕΕΤΤ, ο υπηρεσιακός ιδιοκτήτης του (βλ. ενότητα 3), η ταξινόμηση / διαβάθμιση / κρισιμότητά του (βλ. ενότητα 4), σημαντικά τεχνικά χαρακτηριστικά του, οι πληροφορίες (είδος δεδομένων) που επεξεργάζεται, οι υπηρεσίες που

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

υποστηρίζει, το καθεστώς συντήρησης και αλλαγών, τα τρίτα μέρη που απαιτούνται για τη συντήρηση ή υποστήριξή του και στοιχεία επικοινωνίας αναφορικά με αυτόν.

Προκειμένου να επιτυγχάνει τους σκοπούς του, το Μητρώο Πληροφοριακών Πόρων ενημερώνεται συνεχώς με νέους πληροφοριακούς πόρους που τυχόν προκύπτουν, καθώς και με τις αλλαγές των υφιστάμενων. Πρόσβαση στο Μητρώο έχουν μόνο τα αρμόδια στελέχη λόγω των αρμοδιοτήτων τους.

Ειδικότερα ως προς τις πληροφορίες της, η ΕΕΤΤ ενημερώνει κατ' ελάχιστον σε ετήσια βάση, το Μητρώο με τις κατηγορίες εγγράφων, πληροφοριών και δεδομένων που έχει στην κατοχή της ανά Διεύθυνση ή αυτοτελές Τμήμα και μάλιστα τις διαχωρίζει σε εκείνες που διαθέτει ελεύθερα προς περαιτέρω χρήση και αξιοποίηση για εμπορικούς ή μη εμπορικούς σκοπούς, δηλαδή τα λεγόμενα «ανοικτά δεδομένα» και τις υπόλοιπες πληροφορίες για τις οποίες συντρέχουν περιορισμοί μη δημόσιας διάθεσης (π.χ. δεδομένα προσωπικού χαρακτήρα, απόρρητα κτλ.). Για κάθε κατηγορία τηρεί στοιχεία όπως κωδικό, τίτλο, τυχόν παρατηρήσεις και τους λόγους μη δημοσίευσης/μη δημόσιας διάθεσης, Το ενημερωμένο αυτό Μητρώο Πληροφοριών της ΕΕΤΤ εγκρίνεται με Απόφαση της Ολομέλειάς της.

Η ΕΕΤΤ διατηρεί αυτοματοποιημένο μητρώο υπηρεσιακών υπολογιστών των χρηστών της το οποίο δίνει κατ' ελάχιστον πληροφορίες για το χρήστη του υπολογιστή, το λειτουργικό σύστημα και τα εγκατεστημένα προγράμματα ανά υπολογιστή. Επίσης μπορεί να δοθεί, με τη μορφή αναφοράς, το επίπεδο συμμόρφωσης (patch level) του υπολογιστή σχετικά με τις τελευταίες αναβαθμίσεις λειτουργικού συστήματος.

Οι εγκεκριμένες εφαρμογές για τους υπηρεσιακούς υπολογιστές χρηστών διατηρούνται σε εξειδικευμένο πρόγραμμα διαχείρισης (διαμοιρασμού) λογισμικού. Οποιαδήποτε εγκατάσταση λογισμικού τελεί υπό τον έλεγχο των Προϊσταμένων Οργανικών Μονάδων και της Διεύθυνσης Ψηφιακής Διακυβέρνησης της ΕΕΤΤ.

Για τους εξυπηρετητές της ΕΕΤΤ τηρείται μητρώο το οποίο περιέχει κατ' ελάχιστον πληροφορία για το λειτουργικό σύστημα και το εγκατεστημένο λογισμικό.

2.2 Σήμανση Πληροφοριακών Πόρων

Οι πληροφοριακοί πόροι πρέπει να σημανθούν, έτσι ώστε ένας μοναδικός αναγνωριστικός αριθμός να αντιστοιχεί σε κάθε στοιχείο του μητρώου, εφόσον αυτό είναι εφικτό.

Οι πληροφοριακοί πόροι που υφίστανται σε φυσική μορφή ενδείκνυται να μην έχουν γραπτή σήμανση τοποθετημένη πάνω τους, εάν κριθεί ότι ο άμεσος εντοπισμός τους μπορεί να διευκολύνει τις φυσικές απειλές (π.χ. κλοπή ή καταστροφή).

2.3 Λοιπά Μητρώα συνδεδεμένα με το Μητρώο Πληροφοριακών Πόρων

Με σκοπό την υποστήριξη της υπηρεσιακής δραστηριότητας και της επιτυχούς εφαρμογής των διαδικασιών ασφαλείας, τη συμμόρφωση με το νομοθετικό πλαίσιο, με πρότυπα ασφάλειας και βέλτιστες πρακτικές, καθώς και την παροχή της αναγκαίας λογοδοσίας, η ΕΕΤΤ έχει την ευχέρεια, σύμφωνα με τις εκάστοτε ανάγκες της, να δημιουργεί και να διατηρεί επιπλέον ειδικά μητρώα για τους πληροφοριακούς πόρους της. Τέτοια μητρώα θα μπορούσαν να αφορούν τον προσδιορισμό και την καταγραφή των χρηστών με δικαίωμα πρόσβασης στους πληροφοριακούς πόρους (τόσο σε λογικό, όσο και σε φυσικό επίπεδο), των κινδύνων που απειλούν τους πληροφοριακούς πόρους, των οργανωτικών και τεχνικών μέτρων που εφαρμόζονται για την προστασία τους, των προσθηκών / αλλαγών / βελτιώσεων των πληροφοριακών πόρων, κτλ.

3. Ιδιοκτησία πληροφοριακών πόρων και εξουσιοδότηση για τη χρήση τους

3.1 Ορισμός του ιδιοκτήτη και του θεματοφύλακα των πληροφοριακών πόρων

Κάθε πληροφοριακός πόρος πρέπει να έχει έναν ιδιοκτήτη, ο οποίος είναι ο υπηρεσιακός υπεύθυνος για την εν γένει λειτουργία, ασφάλεια και προστασία του. Ως ιδιοκτήτης στην ΕΕΤΤ νοείται η οργανική μονάδα η οποία έχει την λειτουργική ευθύνη της καθημερινής χρήσης, διαχείρισης και αξιοποίησης του πόρου, σε αντιδιαστολή προς την τεχνική ευθύνη. Με τη λογική αυτή, ιδιοκτήτης των πληροφοριακών συστημάτων και εφαρμογών της ΕΕΤΤ δεν είναι η Διεύθυνση Ψηφιακής Διακυβέρνησης αλλά οι οργανικές μονάδες που είναι λειτουργικά υπεύθυνες και αξιοποιούν τους πόρους κατά την άσκηση των αρμοδιοτήτων τους. Διευκρινίζεται ότι η απαίτηση αυτή για τον ορισμό ιδιοκτήτη, δεν περιορίζεται στα πληροφοριακά συστήματα και εφαρμογές αλλά εκτείνεται στα δεδομένα που διαχειρίζονται, στις υπηρεσιακές πληροφορίες και στα έγγραφα, τόσο σε ψηφιακή όσο και σε φυσική μορφή.

Ο ιδιοκτήτης του πληροφοριακού πόρου οφείλει να αξιολογεί τους κινδύνους που απειλούν τον πόρο και να εξασφαλίζει επαρκή μέτρα για να τον προστατεύσει από απώλεια της εμπιστευτικότητας (δηλαδή μη εξουσιοδοτημένη πρόσβαση), της ακεραιότητας (δηλαδή μη εξουσιοδοτημένη τροποποίηση) και της

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

διαθεσιμότητάς του (δηλαδή απώλεια δεδομένων, απώλεια της πρόσβασης σε αυτά, απώλεια της ψηφιακής συνέχειας).

Ο ιδιοκτήτης του πληροφοριακού πόρου μπορεί να αναθέσει τις σχετικές δραστηριότητες προστασίας των πληροφοριών του, κατά την αποθήκευση, διαχείριση, μεταφορά ή επεξεργασία τους, σε άλλο εξειδικευμένο προσωπικό (το λεγόμενο θεματοφύλακα του πληροφοριακού πόρου), όπως ενδεικτικά στη Διεύθυνση Ψηφιακής Διακυβέρνησης που έχει την απαραίτητη τεχνική γνώση. Ο ιδιοκτήτης του πληροφοριακού πόρου εξακολουθεί να διατηρεί τη συνολική ευθύνη προστασίας του πόρου. Αποτελεί δική του αρμοδιότητα να θέτει τις απαιτήσεις ασφάλειας, να τις ανανεώνει ανάλογα με τις αλλαγές των συνθηκών, να προσαρμόζει τα μέτρα προστασίας σύμφωνα με τις αλλαγές της αξίας της πληροφορίας και των κινδύνων που την απειλούν, να τα επικοινωνεί στους θεματοφύλακες των πληροφοριών και να παρακολουθεί την εφαρμογή τους.

3.2 Συμμόρφωση με την πολιτική διαχείρισης προσβάσεων

Τα δικαιώματα πρόσβασης στους πληροφοριακούς πόρους καθορίζονται από τους ιδιοκτήτες τους, βάσει του επιπέδου ταξινόμησης (βλ. ενότητα 4) και σύμφωνα με τις πολιτικές της ΕΕΤΤ. Πρόσβαση παρέχεται σε εκείνους που την χρειάζονται προκειμένου να εκπληρώσουν τα υπηρεσιακά καθήκοντά τους. Έτσι, πρόσβαση στις εφαρμογές, βάσεις δεδομένων και στα ψηφιακά αρχεία παρέχεται μόνο σε εξουσιοδοτημένους χρήστες. Η πρόσβαση που παρέχεται σε ένα μέλος του προσωπικού λόγω των συγκεκριμένων αρμοδιοτήτων του, καταργείται όταν αυτό μεταφέρεται σε άλλη θέση με άλλες αρμοδιότητες. Η πρόσβαση σε εξοπλισμό που χορηγείται σε έναν εξουσιοδοτημένο χρήστη καταργείται όταν η εργασιακή σχέση του χρήστη με την ΕΕΤΤ ολοκληρώνεται ή όταν ο λογαριασμός του χρήστη είναι ανενεργός.

Υλικό εσωτερικής χρήσης που χρησιμοποιείται αποκλειστικά από συγκεκριμένες οργανικές μονάδες, επιτροπές, ομάδες κτλ. αποθηκεύεται κατάλληλα στο File Server και παρέχεται πρόσβαση μόνο στα μέλη τους. Ενημερώνεται και τηρείται έλεγχος εκδόσεων (versions) στις περιπτώσεις που απαιτείται. Η εκτύπωση του υλικού, εν γένει, αποφεύγεται, όσο είναι αυτό δυνατόν, μεταξύ άλλων και για λόγους ασφαλείας.

Πρόσβαση στους υπηρεσιακούς υπολογιστές των εργαζομένων έχουν μόνο εξουσιοδοτημένα στελέχη της Διεύθυνσης Ψηφιακής Διακυβέρνησης και μόνο μετά από αίτημα του ίδιου του εργαζόμενου.

Η πρόσβαση στο computer room και στα κρίσιμα αρχεία είναι ελεγχόμενη και επιτρέπεται μέσω κάρτας πρόσβασης μόνο στο εξουσιοδοτημένο προσωπικό. Καταγράφονται τα στοιχεία ταυτότητας αυτού που εισήλθε ή εξήλθε, η ημερομηνία και η χρονική στιγμή.

Το λογισμικό αποθηκεύεται (σε φυσική και ψηφιακή μορφή) σε ασφαλή κεντρικό χώρο μαζί με κωδικούς εγκατάστασης και όλο το αναγκαίο συνοδευτικό υλικό και η πρόσβαση σε αυτό περιορίζεται σε εξουσιοδοτημένο προσωπικό μόνο.

Κρίσιμα έγγραφα σε φυσική μορφή (π.χ. με εμπιστευτικές πληροφορίες ή δεδομένα προσωπικού χαρακτήρα) φυλάσσονται, επεξεργάζονται, τηρούνται και καταστρέφονται με ασφαλή τρόπο. Κατά περίπτωση, όπου κρίνεται αναγκαίο, χρησιμοποιείται ενυπόγραφη καταγραφή της πρόσβασης σε αυτά.

Από την άλλη μεριά, υλικό εσωτερικής χρήσης που συνδράμει το προσωπικό της ΕΕΤΤ στην κατανόηση λειτουργιών, διαδικασιών ή συστημάτων αποθηκεύεται στη Γνωσιακή Πύλη (Εστία) και είναι εύκολα προσβάσιμο από όλους τους εργαζόμενους.

Η ΕΕΤΤ χρησιμοποιεί ειδική εφαρμογή που παρέχει στους χρήστες την δυνατότητα αναζήτησης των δικαιωμάτων πρόσβασης στις κυριότερες εφαρμογές της και στα κεντρικά συστήματα, στο file server, στο mail box, στα group emails. Απευθύνεται κυρίως στους προϊσταμένους των οργανικών μονάδων, οι οποίοι υποχρεούνται να ελέγχουν σε τακτική βάση την ορθή παροχή πρόσβασης στα πληροφοριακά συστήματα και τους πόρους της ΕΕΤΤ.

Η πρόσβαση στους πληροφοριακούς πόρους καταγράφεται σε αρχεία καταγραφής και ελέγχεται από εξουσιοδοτημένα στελέχη βάσει της υπηρεσιακής κρισιμότητας του κάθε πόρου. Η απαίτηση αυτή περιλαμβάνει τόσο τον έλεγχο των χρηστών με προνομιακά δικαιώματα πρόσβασης (όπως των διαχειριστών των συστημάτων) όσο και των απλών χρηστών (εργαζομένων της ΕΕΤΤ, αναδόχων, λοιπών τρίτων που έχουν εξουσιοδοτηθεί να έχουν πρόσβαση στους πληροφοριακούς πόρους) (βλ. την ενότητα 4.4 για την ταξινόμηση των χρηστών). Σε κάθε περίπτωση, ο χρήστης δεν έχει την δυνατότητα να αρνηθεί εκ των υστέρων ότι είχε πρόσβαση ή ότι διενήργησε κάποια συναλλαγή στον πληροφοριακό πόρο (non-repudiation).

3.3 Ευθύνες του ιδιοκτήτη πληροφοριακών πόρων

Οι ιδιοκτήτες πληροφοριακών πόρων είναι υπεύθυνοι για τα ακόλουθα:

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

- *Να εξασφαλίζουν ότι έχει γίνει η ταξινόμηση του πόρου σύμφωνα με τις πολιτικές της ΕΕΤΤ (βλ. ενότητα 4 παρακάτω)*
- *Να διασφαλίζουν ότι ο πόρος έχει ταξινομηθεί κατάλληλα ανάλογα με την υπηρεσιακή του αξία*
- *Να εξασφαλίζουν ότι γνωρίζουν το επίπεδο ταξινόμησης των πληροφοριών που εισέρχονται στην ΕΕΤΤ προερχόμενες από τρίτους*
- *Να μεριμνούν ώστε κατ' ελάχιστον τα έγγραφα σε φυσική μορφή να έχουν εμφανώς αναγραμμένο το επίπεδο ταξινόμησης ως προς την εμπιστευτικότητα*
- *Να επιμελούνται την ασφαλή διακίνηση των διαβαθμισμένων πληροφοριών*
- *Να φροντίζουν ώστε το επίπεδο προστασίας του πόρου να είναι ανάλογο με το επίπεδο ταξινόμησής του*
- *Να καθορίζουν τους εξουσιοδοτημένους χρήστες του πόρου και το επιτρεπόμενο επίπεδο πρόσβασης του κάθε χρήστη (όπως απλή ή προνομιακή πρόσβαση)*
- *Να καθορίζουν την καθημερινή διαχείριση του πληροφοριακού πόρου*
- *Να κρατούν το προσωπικό ενήμερο για τις αρμοδιότητές του ως προς τη χρήση του πόρου*
- *Να επιδιώκουν την πλήρη αξιοποίηση του πόρου προς όφελος την υπηρεσίας*
- *Να διασφαλίζουν τη συμμόρφωση με την παρούσα πολιτική*
- *Να αναθέτουν τον πόρο σε θεματοφύλακα, όταν το κρίνουν*
- *Να προβαίνουν σε τακτική αξιολόγηση της ταξινόμησης των πόρων και των δικαιωμάτων πρόσβασης*

4. Ταξινόμηση Πληροφοριακών Πόρων

Ταξινόμηση (ή αλλιώς διαβάθμιση) των πληροφοριακών πόρων είναι η διαδικασία διαχωρισμού και οργάνωσής τους σε ομάδες, βάσει των κοινών χαρακτηριστικών τους, όπως του επιπέδου της ευαισθησίας / κρισιμότητάς τους, των κινδύνων που τους απειλούν ή της νομοθεσίας και των κανονισμών που τους προστατεύουν.

Η ΕΕΤΤ πρέπει να ταξινομεί τους πληροφοριακούς πόρους της, καθώς η ταξινόμηση τής επιτρέπει να κατανοεί τους διαφορετικούς τύπους πληροφορίας που επεξεργάζεται και αποθηκεύει και να λαμβάνει τα απαραίτητα μέτρα προστασίας για τον κάθε τύπο πληροφορίας και το κάθε πληροφοριακό σύστημα, σύμφωνα με τη σημαντικότητα, κρισιμότητα και ευαισθησία του. Όσο πιο κρίσιμη είναι μια πληροφορία, μία εφαρμογή ή ένα σύστημα, τόσο πιο αυστηρά μέτρα ασφάλειας απαιτούνται για την προστασία τους.

Η ΕΕΤΤ διαθέτει ένα δομημένο σύστημα ταξινόμησης πληροφοριακών πόρων, το οποίο αναθεωρείται και προσαρμόζεται στις υπηρεσιακές ανάγκες, όπως αυτές οι ανάγκες ενδέχεται να μεταβάλλονται. Το σύστημα ταξινόμησης της ΕΕΤΤ περιγράφει τον τρόπο που η ΕΕΤΤ κατηγοριοποιεί τους πληροφοριακούς πόρους της, με βάση την κρισιμότητά τους, λαμβάνοντας υπόψη, δηλαδή, τις εκτιμώμενες συνέπειες (απτές και μη) σε περίπτωση παραβίασης της ασφάλειάς τους. Πιο συγκεκριμένα, προσδιορίζει και τεκμηριώνει τα επίπεδα ταξινόμησης (με εύρος που εκτείνεται από το υψηλότερο προς το χαμηλότερο επίπεδο) και τα κριτήρια που καθορίζουν την ένταξη των πληροφοριών, εφαρμογών, δικτύων, πληροφοριακών συστημάτων της, σε αυτά τα επίπεδα ταξινόμησης, σύμφωνα με τις τρεις (3) αρχές της ασφάλειας πληροφοριών, δηλαδή την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα.

Η ταξινόμηση των πληροφοριακών πόρων προϋποθέτει και ξεκινά με την ταξινόμηση των πληροφοριών που κατέχει η ΕΕΤΤ και υποστηρίζουν τις λειτουργίες της (βλ. ενότητα 4.1). Κατόπιν, ακολουθεί η ταξινόμηση των υπόλοιπων πληροφοριακών πόρων με βάση τις πληροφορίες τους (βλ. ενότητα 4.2).

4.1 Ταξινόμηση Πληροφοριών

Οι πληροφορίες, ανεξάρτητα από τη μορφή που έχουν (όπως πληροφορίες σε φυσική μορφή, αποθηκευμένες ηλεκτρονικά ή μεταφερόμενες με ηλεκτρονικά μέσα) εκτίθενται σε απειλές. Η έλλειψη ενημέρωσης του προσωπικού ή η περιστασιακή παροχή πληροφοριών για την προστασία τους μπορεί να έχει ως αποτέλεσμα αυξημένους κινδύνους για τις υπηρεσίες ενός Οργανισμού.

Οι πληροφορίες που κατέχει η ΕΕΤΤ πρέπει να παραμένουν ακριβείς, διαθέσιμες και επαρκώς προστατευμένες, διότι όλες έχουν αξία. Όμως δεν απαιτούν όλες οι πληροφορίες το ίδιο επίπεδο προστασίας, καθώς δεν έχουν

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

όλες την ίδια υπηρεσιακή αξία. Η ταξινόμηση των πληροφοριών στοχεύει ακριβώς στην εκτίμηση της αξία τους, που είναι καίρια για τον προσδιορισμό του επιπέδου ασφαλείας που απαιτούν.

Για το σκοπό αυτό, καταρχάς, αναγνωρίζονται και καταγράφονται οι διαφορετικοί τύποι πληροφοριών που υποστηρίζουν τις διάφορες λειτουργίες της ΕΕΤΤ. Ακολουθεί η ταξινόμησή τους βάσει του συστήματος ταξινόμησης. Με το σύστημα ταξινόμησης της ΕΕΤΤ, οι πληροφορίες διαβαθμίζονται στα επίπεδα ταξινόμησης με βάση τις αρχές ασφάλειας πληροφοριών, δηλαδή το πόσο ευαίσθητες είναι σε σχέση με την εμπιστευτικότητα (αποκάλυψη σε μη εξουσιοδοτημένα πρόσωπα), την ακεραιότητα (τροποποίηση από μη εξουσιοδοτημένα πρόσωπα) και την διαθεσιμότητά τους.

Όπως έχει ήδη αναφερθεί, η ταξινόμηση των πληροφοριών είναι ευθύνη των υπηρεσιακών ιδιοκτητών τους και επισημαίνεται ότι πρέπει να διενεργείται βάσει της αξίας που έχει η κάθε πληροφορία για την ίδια την ΕΕΤΤ και όχι για τυχόν άλλα πρόσωπα ή φορείς από τους οποίους προέρχεται ή στους οποίους κατευθύνεται.

4.1.1 Ταξινόμηση της πληροφορίας με βάση την εμπιστευτικότητα

Οι πληροφορίες ταξινομούνται, καταρχήν, σύμφωνα με τον αντίκτυπο που θα έχει η αποκάλυψή τους σε μη εξουσιοδοτημένα πρόσωπα.

Πιο συγκεκριμένα, καθορίζονται τα παρακάτω επίπεδα ταξινόμησης ως προς την εμπιστευτικότητα:

Ταξινόμηση πληροφοριών με βάση την εμπιστευτικότητα			
Ταξινόμηση		**Επίπεδο**	**Περιγραφή**
ΑΚΡΩΣ ΑΠΟΡΡΗΤΑ	**ΑΚΡΩΣ ΥΨΗΛΗ**	**5**	*Ο χαρακτηρισμός αυτός δίδεται σε πληροφορίες οι οποίες εάν αποκαλυφθούν σε μη εξουσιοδοτημένο προσωπικό, είναι δυνατό να προκαλέσουν σοβαρές ζημιές στην Εθνική Άμυνα και ασφάλεια της χώρας, καθώς και στα ζωτικά της συμφέροντα.* *Πρόσβαση σε αυτές έχουν, κατά κύριο λόγο, διαπιστευμένα πρόσωπα, ενδεικτικά τα στελέχη της ομάδας Πολιτικού Σχεδιασμού Εκτάκτου Ανάγκης (ΠΣΕΑ) της ΕΕΤΤ, τα οποία τις διαχειρίζονται κατάλληλα με πλήρη εχεμύθεια και εμπιστευτικότητα. Λαμβάνονται άκρως αυστηρά μέτρα φυσικής και λογικής ασφάλειας.*
ΑΠΟΡΡΗΤΑ	**ΠΟΛΥ ΥΨΗΛΗ**	**4**	*Ο χαρακτηρισμός αυτός δίδεται σε πληροφορίες οι οποίες αφορούν ευαίσθητα δεδομένα τα οποία πρέπει να είναι προσβάσιμα μόνο από πολύ περιορισμένο πλήθος ατόμων που τα χρειάζονται για την εκτέλεση των εργασιών τους. Η μη εξουσιοδοτημένη πρόσβαση σε αυτά θα είχε σημαντικό αρνητικό αντίκτυπο στην εικόνα ή / και στη λειτουργία της ΕΕΤΤ.* *Ενδεικτικά παραδείγματα αποτελούν οι πληροφορίες για την αυθεντικοποίηση των στελεχών της ΕΕΤΤ, οι κωδικοί πρόσβασης (passwords), η τεκμηρίωση των ρυθμίσεων ασφαλείας των πληροφοριακών συστημάτων, τα κλειδιά κρυπτογράφησης κτλ.* *Η διαχείριση αυτής της πληροφορίας πρέπει να είναι ελεγχόμενη σε συνεχή βάση. Ο ιδιοκτήτης της πληροφορίας πρέπει να γνωρίζει ανά πάσα στιγμή ποιος έχει πρόσβαση στην απόρρητη πληροφορία. Έτσι, πρέπει να τηρείται σχετική καταγραφή προσβάσεων (logging), η οποία θα ελέγχεται*

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

			τακτικά. Οι απόρρητες πληροφορίες πρέπει να αποθηκεύονται και διαβιβάζονται με ασφάλεια (π.χ. με κρυπτογράφηση).
ΕΜΠΙΣΤΕΥΤΙΚΑ	***ΥΨΗΛΗ***	***3***	*Αυτή η κατηγορία αφορά τις πληροφορίες που δεν χαρακτηρίζονται ως απόρρητες αλλά αφορούν ευαίσθητα δεδομένα που πρέπει να είναι προσβάσιμα με εμπιστευτικότητα μόνο από άτομα που έχουν ανάγκη από αυτά για την εκτέλεση των εργασιών τους. Απαιτούν υψηλού βαθμού τεχνικά και οργανωτικά μέτρα ασφαλείας. Η μη εξουσιοδοτημένη πρόσβαση σε αυτά θα είχε σημαντικό αρνητικό αντίκτυπο στην εικόνα ή / και λειτουργία της ΕΕΤΤ και/ή στους εργαζόμενους, τους συνεργάτες, τις εποπτευόμενες αγορές και/ή τους πολίτες.* *Παραδείγματα τέτοιων πληροφοριών είναι κάθε εισερχόμενη αλληλογραφία που κρίνεται από την ΕΕΤΤ εμπιστευτική, οικονομικά και λοιπά εμπιστευτικά στοιχεία των παρόχων, τα πορίσματα των ελέγχων των παρόχων, οι εκθέσεις των εσωτερικών ελέγχων, τα πρακτικά των συνεδριάσεων της Ολομέλειας, πληροφορίες για νομικές υποθέσεις (π.χ. ακροάσεις, εκδικάσεις), εμπιστευτικές μελέτες, περιστατικά και αναφορές ασφαλείας, τεκμηρίωση των πληροφοριακών συστημάτων, κτλ. Τα δεδομένα προσωπικού χαρακτήρα επίσης ανήκουν σε αυτήν τη κατηγορία.* *Εμπιστευτικές πληροφορίες πρέπει να διανέμονται εσωτερικά μόνο σε συγκεκριμένους εξουσιοδοτημένους αποδέκτες. Δεν επιτρέπεται η πρόσβαση ή κοινοποίηση σε μη εξουσιοδοτημένα άτομα εντός και εκτός ΕΕΤΤ χωρίς την έγκριση του ιδιοκτήτη της πληροφορίας.* *Τα ηλεκτρονικά εμπιστευτικά δεδομένα πρέπει να προστατεύονται μέσω κωδικού πρόσβασης ή να είναι προστατευμένα στο επίπεδο βάσεων δεδομένων ή / και στο επίπεδο των εφαρμογών. Εμπιστευτική πληροφορία σε ηλεκτρονική μορφή δεν πρέπει να εκτυπώνεται ή να αποστέλλεται με ηλεκτρονικά μέσα χωρίς μέτρα ασφαλείας.* *Εμπιστευτικά δεδομένα σε φυσική μορφή πρέπει να προστατεύονται με φυσικά μέτρα ασφάλειας (κλείδωμα σε φωριαμούς, διακίνηση σε κλειστούς φακέλους κτλ.). Η εμπιστευτική πληροφορία σε φυσική μορφή δεν πρέπει να σαρώνεται ή να φωτοτυπείται χωρίς μέτρα ασφαλείας.* *Επίσης, ιδιαίτερη προσοχή δίνεται στην περίπτωση χειρισμού εμπιστευτικών πληροφοριών σε δημόσιους χώρους. Για παράδειγμα, συζητήσεις μέσω τηλεφώνου για εμπιστευτικές πληροφορίες πρέπει να αποφεύγονται.* *Η διακίνηση των εμπιστευτικών εγγράφων γίνεται στην ΕΕΤΤ μέσω του εμπιστευτικού πρωτοκόλλου του Συστήματος*

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

			Ηλεκτρονικής Διαχείρισης Εγγράφων (ΣΗΔΕ), ακολουθώντας αυστηρά μέτρα προστασίας και σύμφωνα με τον Κανονισμό Λειτουργίας της ΕΕΤΤ, όπως έχει τροποποιηθεί και ισχύει. Έτσι, αυστηρά μόνο τα συγκεκριμένα στελέχη που πρέπει να γνωρίζουν λόγω αρμοδιότητας αποκτούν πρόσβαση.
ΕΣΩΤΕΡΙΚΗΣ ΧΡΗΣΗΣ	***ΜΕΣΑΙΑ***	***2***	*Αυτό το επίπεδο ταξινόμησης αφορά τις πληροφορίες που πρόκειται να χρησιμοποιηθούν εσωτερικά στην ΕΕΤΤ. Δεν εντάσσονται στις άλλες κατηγορίες των απορρήτων και εμπιστευτικών πληροφοριών και διανέμονται μεταξύ του προσωπικού υπό τον έλεγχο του ιδιοκτήτη τους.* *Η μη εξουσιοδοτημένη αποκάλυψη/διαβίβαση αυτών των πληροφοριών εκτός ΕΕΤΤ απαγορεύεται εκτός αν επιτραπεί ρητώς από τον ιδιοκτήτη.* *Παραδείγματα τέτοιων πληροφοριών είναι το υλικό από εσωτερικές εκπαιδεύσεις, έγγραφα εσωτερικής αλληλογραφίας, εσωτερικές πολιτικές και διαδικασίες, υπηρεσιακά σημειώματα, ενδοτμηματικές αναφορές, κλπ.* *Τα έγγραφα εσωτερικής χρήσης διακινούνται στο Σύστημα Ηλεκτρονικής Διαχείρισης Εγγράφων (ΣΗΔΕ) ως εσωτερικά έγγραφα και μπορούν να αναρτώνται στη Γνωσιακή Πύλη (εστία) της ΕΕΤΤ για ενημέρωση του προσωπικού.* *Η πληροφορία εσωτερικής χρήσης πρέπει να καταστρέφεται με ασφαλή τρόπο σύμφωνα με τις ενδείξεις του ιδιοκτήτη της.*
ΔΗΜΟΣΙΑ ΠΛΗΡΟΦΟΡΙΑ (αδιαβάθμητα)	***ΧΑΜΗΛΗ***	***1***	*Πρόκειται για αδιαβάθμητη πληροφορία για την οποία υπάρχει ανάγκη πρόσβασης από ευρύ κοινό (π.χ. παρόχους, καταναλωτές, πολίτες κτλ.) και δημιουργείται με στόχο την δημόσια χρήση και διάθεση από τον ιδιοκτήτη της.* *Αυτό το επίπεδο ταξινόμησης αφορά πληροφορίες που θα επικοινωνηθούν στο κοινό από εξουσιοδοτημένους εργαζόμενους. Δεν υπάρχει εξ ορισμού απειλή από την αποκάλυψη αυτών των πληροφοριών και μπορούν να κυκλοφορούν ελεύθερα χωρίς κανένα πιθανό αντίκτυπο.* *Παραδείγματα τέτοιων πληροφοριών είναι οι ανακοινώσεις, τα δελτία τύπου, οι εκδόσεις και τα ενημερωτικά φυλλάδια της ΕΕΤΤ κλπ. Τα ανοικτά δεδομένα επίσης ανήκουν σε αυτήν τη κατηγορία.* *Πρόσβαση στη δημόσια πληροφορία μπορούν να έχουν όλα τα στελέχη της ΕΕΤΤ αλλά και οιοσδήποτε τρίτος ενδιαφερόμενος. Επομένως, η πληροφορία αναρτάται στον διαδικτυακό τόπο της ΕΕΤΤ ή δημοσιεύεται με άλλους τρόπους από εξουσιοδοτημένα*

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

			στελέχη, μετά από έγκριση, σύμφωνα με τις τυποποιημένες διαδικασίες δημοσίευσης της ΕΕΤΤ. *Πριν την επίσημη δημοσίευση κάθε τέτοια πληροφορία πρέπει να προστατεύεται, αλλά δεν απαιτείται καμία προφύλαξη ασφαλείας για να προστατευθεί η εμπιστευτικότητα της πληροφορίας μετά τη δημοσίευσή της. Επίσης, δεν απαιτείται ασφαλής μέθοδος για την καταστροφή της πληροφορίας. Αντιθέτως, κατά την περίοδο διατήρησης της πληροφορίας, απαιτούνται μέτρα για την προστασία της ακεραιότητας και διαθεσιμότητάς της.*

Ο συντάκτης ενός εγγράφου που συντάσσεται στην ΕΕΤΤ είναι αρμόδιος για την ταξινόμηση και τον χαρακτηρισμό του ως προς την εμπιστευτικότητα. Από εκεί και πέρα, οι υπάλληλοι της ΕΕΤΤ και οι τρίτοι που λαμβάνουν το έγγραφο, πρέπει να το χειρίζονται με τη δέουσα προσοχή και με τρόπο που να συνάδει με την ταξινόμησή του.

Αναφορικά με τα εισερχόμενα, στην ΕΕΤΤ, έγγραφα μπορεί να έχουν χαρακτηριστεί εμπιστευτικά από τους αποστολείς τους για τους δικούς του λόγους, αλλά εφ' όσον ο αποστολέας δεν είναι δημόσια αρχή, η ΕΕΤΤ έχει το δικαίωμα να επανεκτιμήσει την ταξινόμησή τους κι αν κρίνει ότι δεν πρόκειται για διαβαθμισμένα έγγραφα να τα χειριστεί κατάλληλα ως μη διαβαθμισμένα.

4.1.2 Ταξινόμηση της πληροφορίας με βάση την ακεραιότητα

Οι πληροφορίες ταξινομούνται, επίσης, σύμφωνα με τον αντίκτυπο που θα έχει η τυχαία ή μη εξουσιοδοτημένη τροποποίησή τους. Πιο συγκεκριμένα, ορίζονται τα παρακάτω επίπεδα ταξινόμησης ως προς την ακεραιότητα:

Ταξινόμηση πληροφοριών με βάση την ακεραιότητά τους		
Ταξινόμηση	***Επίπεδο***	***Περιγραφή***
ΥΨΗΛΗ	***3***	*Οι κρίσιμες υπηρεσιακές λειτουργίες εξαρτώνται από αυτές τις πληροφορίες και την υποδομή που χρησιμοποιείται για την επεξεργασία των πληροφοριών. Η μη εξουσιοδοτημένη τροποποίηση των πληροφοριών μπορεί να έχει ανεπανόρθωτες επιπτώσεις στους παρόχους, τις αγορές που εποπτεύει η ΕΕΤΤ, τους πολίτες, τους συνεργάτες, τους εργαζόμενους, τις λειτουργίες της ΕΕΤΤ.*
ΜΕΣΑΙΑ	***2***	*Σημαντικές υπηρεσιακές λειτουργίες βασίζονται στις πληροφορίες αυτού του είδους και στην υποδομή που χρησιμοποιείται για την επεξεργασία των πληροφοριών. Η μη εξουσιοδοτημένη τροποποίηση των πληροφοριών μπορεί να έχει σοβαρές αλλά αναστρέψιμες επιπτώσεις.*
ΧΑΜΗΛΗ	***1***	*Οι υπηρεσιακές λειτουργίες της ΕΕΤΤ δεν βασίζονται σε αυτές τις πληροφορίες και την υποδομή που χρησιμοποιείται για την επεξεργασία τους. Η μη εξουσιοδοτημένη τροποποίηση του περιεχομένου τους αναμένεται να έχει περιορισμένες επιπτώσεις (δηλαδή μέσα σε αποδεκτά όρια) ή να μην έχει καθόλου αρνητικό αντίκτυπο στην ΕΕΤΤ.*

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

4.1.3 Ταξινόμηση της πληροφορίας με βάση την διαθεσιμότητα

Οι πληροφορίες ταξινομούνται, επίσης, σύμφωνα με τον αντίκτυπο που θα έχει η μη διαθεσιμότητά τους.

Πιο συγκεκριμένα, πληροφορίες που τηρούνται ηλεκτρονικά πρέπει να ταξινομούνται λαμβάνοντας υπόψη τα παρακάτω:

- *Το χρονικό διάστημα εντός του οποίου πρέπει να είναι διαθέσιμες οι πληροφορίες (Στόχος χρόνου ανάκτησης).*
- *Πόσο ενημερωμένα πρέπει να είναι τα αντίγραφα ασφαλείας (backups) (Στόχος σημείου ανάκτησης).*

Στόχος Χρόνου Ανάκτησης (Recovery Time Objective/RTO): Ο χρόνος εντός του οποίου θα πρέπει να ανακτηθούν οι πληροφορίες		
Ταξινόμηση	***Επίπεδο***	***Περιγραφή***
ΠΟΛΥ ΥΨΗΛΗ	***5***	*Τα δεδομένα πρέπει να ανακτηθούν εντός **4 ωρών**.*
ΥΨΗΛΗ	***4***	*Τα δεδομένα πρέπει να ανακτηθούν εντός **24 ωρών**.*
ΜΕΣΑΙΑ	***3***	*Τα δεδομένα πρέπει να ανακτηθούν εντός **48 ωρών**.*
ΧΑΜΗΛΗ	***2***	*Τα δεδομένα πρέπει να ανακτηθούν εντός **2 με 5 ημέρες**.*
ΠΟΛΥ ΧΑΜΗΛΗ	***1***	*Τα δεδομένα πρέπει να ανακτηθούν εντός **6 με 30 ημέρες**.*

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

Στόχος Σημείου Ανάκτησης (Recovery Point Objective/RPO): Πόσο ενημερωμένα πρέπει να είναι τα αντίγραφα ασφαλείας		
Ταξινόμηση	***Επίπεδο***	***Περιγραφή***
ΠΟΛΥ ΥΨΗΛΗ	*5*	*Τα αντίγραφα ασφάλειας πρέπει να ενημερώνονται με δεδομένα των τελευταίων **4 ωρών.***
ΥΨΗΛΗ	*4*	*Τα αντίγραφα ασφάλειας πρέπει να ενημερώνονται με δεδομένα των τελευταίων **24 ωρών.***
ΜΕΣΑΙΑ	*3*	*Τα αντίγραφα ασφάλειας πρέπει να ενημερώνονται με δεδομένα των τελευταίων **48 ωρών.***
ΧΑΜΗΛΗ	*2*	*Τα αντίγραφα ασφάλειας πρέπει να ενημερώνονται με δεδομένα των τελευταίων **2 με 5 ημερών.***
ΠΟΛΥ ΧΑΜΗΛΗ	*1*	*Τα αντίγραφα ασφάλειας πρέπει να ενημερώνονται με δεδομένα των τελευταίων **6 με 30 ημερών.***

4.1.4 Κρισιμότητα των πληροφοριών

Οι πληροφορίες ταξινομούνται συνολικά ανάλογα με την κρισιμότητά τους, η οποία προκύπτει από το επίπεδο ταξινόμησης που τους αποδίδεται συνδυαστικά για την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα.

Ειδικότερα, εάν τουλάχιστον μία ταξινόμηση από τις ταξινομήσεις για εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα είναι κατ' ελάχιστον υψηλή (δηλαδή είναι άκρως υψηλή ή πολύ υψηλή ή υψηλή), τότε η πληροφορία είναι κρίσιμη.

Αντιθέτως, εάν όλες οι ταξινομήσεις για εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα είναι κατά μέγιστο χαμηλές (δηλαδή είναι χαμηλές ή πολύ χαμηλές), τότε η πληροφορία είναι μη κρίσιμη.

Στις υπόλοιπες περιπτώσεις, η πληροφορία είναι ευαίσθητη.

Με τον παραπάνω τρόπο, κάθε πληροφορία αποκτά ένα μοναδικό και συγκεκριμένο επίπεδο κρισιμότητας, δηλαδή χαρακτηρίζεται «Κρίσιμη» ή «Ευαίσθητη» ή «Μη κρίσιμη».

Σύμφωνα με τα οριζόμενα στην παρούσα πολιτική, η ΕΕΤΤ προσδιορίζει για κάθε είδος πληροφορίας που κατέχει το επίπεδο κρισιμότητάς του (βλ. Παράρτημα Α) και στη συνέχεια βάσει αυτού καθορίζει και τα μέτρα ασφαλείας που πρέπει να λαμβάνει για την συγκεκριμένη πληροφορία. Όσο πιο κρίσιμη είναι μια πληροφορία, τόσο πιο αυστηρά μέτρα ασφάλειας απαιτούνται για την προστασία της.

4.1.5 Επιπλέον δεικτοδότηση της πληροφορίας λόγω νομικών απαιτήσεων

Επιπλέον του αποδιδόμενου επιπέδου κρισιμότητας, που περιγράφηκε παραπάνω, οι πληροφορίες λαμβάνουν μια ειδική ένδειξη σύμφωνα με τις νομικές απαιτήσεις που τις επηρεάζουν, π.χ. συμμόρφωση με τη νομοθεσία για τα δεδομένα προσωπικού χαρακτήρα, συμμόρφωση με τη νομοθεσία για τα ανοικτά δεδομένα, κτλ. Η ένδειξη αυτή είναι σημαντική για τη διαχείρισή τους σύμφωνα με το αντίστοιχο νομοθετικό πλαίσιο.

Συγκεκριμένα, οι εμπιστευτικές πληροφορίες που περιέχουν προσωπικά δεδομένα (σύμφωνα με το Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ) και το Ν. 4624/2019 όπως ισχύει και ενδεχομένως σύμφωνα με πρότερη διαβούλευση με τον Υπεύθυνο Προστασίας Δεδομένων / DPO της ΕΕΤΤ) λαμβάνουν την επιπλέον ένδειξη «Προσωπικά Δεδομένα» και πρέπει να συμμορφώνονται με το νομοθετικό πλαίσιο για τα προσωπικά δεδομένα.

Οι δημόσιες πληροφορίες που διατίθενται ως ανοικτά δεδομένα (σύμφωνα με το Ν. 4727/2020 όπως ισχύει και την εκάστοτε ισχύουσα απόφαση της ΕΕΤΤ) λαμβάνουν την επιπλέον ένδειξη «Ανοικτά Δεδομένα» και πρέπει να συμμορφώνονται με το νομοθετικό πλαίσιο για τα ανοικτά δεδομένα.

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

Η ΕΕΤΤ ενδέχεται να προσθέσει και άλλες ενδείξεις, όπως οι δύο παραπάνω, στις πληροφορίες της, όπως θα το κρίνει, σύμφωνα με νέες νομικές απαιτήσεις που μπορεί να προκύψουν και με απώτερο σκοπό τη διευκόλυνση της διαχείρισής τους.

4.2 Ταξινόμηση πληροφοριακών πόρων με βάση τις πληροφορίες τους

Σε συνέχεια της ταξινόμησης των πληροφοριών, ακολουθεί η ταξινόμηση των πληροφοριακών πόρων. Δηλαδή όλοι οι πληροφοριακοί πόροι ταξινομούνται από τους ιδιοκτήτες τους στα κατάλληλα επίπεδα, με βάση την ταξινόμηση των πληροφοριών τους. Ειδικότερα:

- *Εφαρμογές*: Κάθε εφαρμογή της ΕΕΤΤ ταξινομείται σύμφωνα με το επίπεδο ταξινόμησης των πληροφοριών που η εφαρμογή επεξεργάζεται ή αποθηκεύει.

- *Πληροφοριακά Συστήματα*: Κάθε πληροφοριακό σύστημα της ΕΕΤΤ ταξινομείται σύμφωνα με τα επίπεδα ταξινόμησης των εφαρμογών που φιλοξενούνται σε αυτό και των συστημάτων και δικτύων στα οποία αυτό συνδέεται άμεσα ή από τα οποία εξαρτάται.

- *Δίκτυα*: Κάθε δίκτυο της ΕΕΤΤ ταξινομείται με βάση τα επίπεδα ταξινόμησης των δικτύων με τα οποία συνδέεται (π.χ. εξωτερικά δημόσια ή ιδιωτικά δίκτυα, εσωτερικά δίκτυα κ.λ.π.) και των πληροφοριακών συστημάτων εντός του δικτύου. Επιπλέον, δίκτυα με το ίδιο επίπεδο ταξινόμησης ταξινομούνται περαιτέρω με βάση το διαφορετικό επίπεδο απειλών για τα συστήματα και τα δεδομένα που μεταφέρονται εντός αυτών των δικτύων.

- *Συστήματα Ασφαλείας / Συσκευές Δικτύου*: Κάθε σύστημα / υποδομή ασφαλείας και συσκευή δικτύου ταξινομείται σύμφωνα με το επίπεδο ταξινόμησης του δικτύου που ανήκει ή των επιπέδων ταξινόμησης των δικτύων που συνδέεται.

- *Λοιπός εξοπλισμός που αποθηκεύει ή επεξεργάζεται δεδομένα, π.*χ. φορητά μέσα για την αποθήκευση πληροφοριών: Λαμβάνουν το κατάλληλο επίπεδο ταξινόμησης σύμφωνα με την ταξινόμηση της πληροφορίας που περιλαμβάνουν και αναλόγως φυλάσσονται σε ασφαλή τοποθεσία. Φορητά μέσα που δεν χρησιμοποιούνται πλέον, πρέπει να διαχειρίζονται με ασφάλεια.

Τα παραπάνω αναλύονται στις επόμενες ενότητες.

4.2.1 Ταξινόμηση των εφαρμογών

Το επίπεδο ταξινόμησης το οποίο αποδίδεται σε μια εφαρμογή προκύπτει αφού ληφθούν υπόψη όλες οι παράμετροι για την ταξινόμηση πληροφοριών, όπως αναλύονται στις προηγούμενες ενότητες. Έτσι, με δεδομένο ότι το σύνηθες είναι μία εφαρμογή να επεξεργάζεται και αποθηκεύει παράλληλα πολλά διαφορετικά είδη πληροφορίας (π.χ. προσωπικά δεδομένα, άλλες εμπιστευτικές πληροφορίες, ανοικτά δεδομένα κτλ.), προκειμένου να εξαχθεί η κρισιμότητα μιας εφαρμογής της ΕΕΤΤ ως προς την εμπιστευτικότητα, ακεραιότητα ή διαθεσιμότητα, πρέπει πρώτα να εκτιμηθεί η ταξινόμηση ως προς την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, αντίστοιχα, κάθε διαφορετικού είδους πληροφορίας (συνόλου δεδομένων) που επεξεργάζεται ή αποθηκεύει η εφαρμογή.

Στη συνέχεια, η εφαρμογή ταξινομείται ως προς την εμπιστευτικότητα, ακεραιότητα ή διαθεσιμότητα σύμφωνα με την εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, αντίστοιχα, συνδυαστικά του συνόλου των πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή αυτή (βλ. Παράρτημα Α).

*Συγκεκριμένα, **ως προς την εμπιστευτικότητα της εφαρμογής:***

Μια εφαρμογή χαρακτηρίζεται ως «κρίσιμη ως προς την εμπιστευτικότητα» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την εμπιστευτικότητα των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι κατ' ελάχιστον η υψηλή ταξινόμηση (δηλαδή είναι άκρως υψηλή ή πολύ υψηλή ή υψηλή ταξινόμηση).*

Μια εφαρμογή χαρακτηρίζεται ως «ευαίσθητη ως προς την εμπιστευτικότητα» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την εμπιστευτικότητα των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι η μεσαία ταξινόμηση.*

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

Μια εφαρμογή χαρακτηρίζεται ως «μη κρίσιμη ως προς την εμπιστευτικότητα» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την εμπιστευτικότητα των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι η χαμηλή ταξινόμηση.*

Ως προς την ακεραιότητα της εφαρμογής:

Μια εφαρμογή χαρακτηρίζεται ως «κρίσιμη ως προς την ακεραιότητα» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την ακεραιότητα των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι η υψηλή ταξινόμηση.*

Μια εφαρμογή χαρακτηρίζεται ως «ευαίσθητη ως προς την ακεραιότητα» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την ακεραιότητα των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι η μεσαία ταξινόμηση.*

Μια εφαρμογή χαρακτηρίζεται ως «μη κρίσιμη ως προς την ακεραιότητα» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την ακεραιότητα των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι η χαμηλή ταξινόμηση.*

***Ως προς την διαθεσιμότητα της εφαρμογής ως προς το χρόνο ανάκτησης** (RTO):*

Μια εφαρμογή χαρακτηρίζεται «κρίσιμη ως προς το χρόνο ανάκτησης» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την διαθεσιμότητα RTO των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι κατ' ελάχιστον η υψηλή ταξινόμηση (δηλαδή είναι πολύ υψηλή ή υψηλή ταξινόμηση).*

Μια εφαρμογή χαρακτηρίζεται «ευαίσθητη ως προς το χρόνο ανάκτησης» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την διαθεσιμότητα RTO των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι η μεσαία ταξινόμηση.*

Μια εφαρμογή χαρακτηρίζεται «μη κρίσιμη ως προς το χρόνο ανάκτησης» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την διαθεσιμότητα RTO των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι κατά μέγιστο η χαμηλή ταξινόμηση (δηλαδή είναι είτε η χαμηλή είτε η πολύ χαμηλή ταξινόμηση).*

***Ως προς την διαθεσιμότητα της εφαρμογής ως προς το σημείο ανάκτησης** (RPO):*

Μια εφαρμογή χαρακτηρίζεται «κρίσιμη ως προς το σημείο ανάκτησης» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την διαθεσιμότητα RPO των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι κατ' ελάχιστον η υψηλή ταξινόμηση (δηλαδή είναι η πολύ υψηλή ή η υψηλή ταξινόμηση).*

Μια εφαρμογή χαρακτηρίζεται «ευαίσθητη ως προς το σημείο ανάκτησης» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την διαθεσιμότητα RPO των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι η μεσαία ταξινόμηση.*

Μια εφαρμογή χαρακτηρίζεται «μη κρίσιμη ως προς το σημείο ανάκτησης» αν το παρακάτω είναι αληθές:

- *Το υψηλότερο επίπεδο ταξινόμησης ως προς την διαθεσιμότητα RPO των διαφορετικών ειδών πληροφοριών που υφίστανται επεξεργασία ή αποθηκεύονται στην εφαρμογή είναι κατά μέγιστο η χαμηλή ταξινόμηση (δηλαδή είναι είτε η χαμηλή είτε η πολύ χαμηλή ταξινόμηση).*

Η ΕΕΤΤ οφείλει να ταξινομεί τις εφαρμογές της, σύμφωνα με τα παραπάνω οριζόμενα στην παρούσα πολιτική. Προσδιορίζει για κάθε εφαρμογή τα τρία επίπεδα κρισιμότητας ως προς την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα (βλ. Παράρτημα Α) και στη συνέχεια βάσει αυτών καθορίζει και τα μέτρα ασφαλείας που πρέπει να λαμβάνει αντίστοιχα για την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα της εφαρμογής. Όσο πιο κρίσιμη είναι μια εφαρμογή, τόσο πιο αυστηρά μέτρα ασφάλειας απαιτούνται για την προστασία της.

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

4.2.2 Ταξινόμηση της διασυνδεσιμότητας των πληροφοριακών συστημάτων

Η ταξινόμηση των πληροφοριακών συστημάτων επηρεάζεται από την κατηγορία δικτύων στην οποία είναι συνδεδεμένα. Η βασική κατηγοριοποίηση που ακολουθείται για τα δίκτυα είναι:

- *Εξωτερικά Δημόσια Δίκτυα: Υπάρχουν δίκτυα που δεν εμπίπτουν στη σφαίρα επιρροής ή αρμοδιότητας της ΕΕΤΤ (π.χ. το διαδίκτυο). Έτσι, η ΕΕΤΤ δεν έχει ευθύνη για τη διαχείριση και συντήρηση αυτών των δικτύων. Αυτά τα δίκτυα είναι εξ ορισμού «μη αξιόπιστα».*
- *Εξωτερικά Ιδιωτικά Δίκτυα: Αυτά τα δίκτυα, αν και είναι ιδιωτικά, δεν εμπίπτουν στη σφαίρα επιρροής και ευθύνης της ΕΕΤΤ (π.χ. δίκτυα συνεργατών). Επομένως, η ΕΕΤΤ δεν έχει ευθύνη για τη διαχείριση και συντήρηση αυτών των δικτύων. Αυτά τα δίκτυα μπορεί να θεωρούνται «ημί-αξιόπιστα», λόγω του γεγονότος ότι είναι ιδιωτικά, με τον όρο ότι η σύμβαση μεταξύ ΕΕΤΤ και εμπλεκόμενου τρίτου είναι σύμφωνη με την σχετική πολιτική.*
- *Δίκτυα Εξωτερικών Υπηρεσιών: Αυτά είναι δίκτυα που περιέχουν πληροφοριακά συστήματα που παρέχουν τις υπηρεσίες της ΕΕΤΤ σε εξωτερικά δίκτυα (π.χ. υποδομή διαδικτύου που υποστηρίζει ιστοτόπους, ηλεκτρονικό ταχυδρομείο κ.λ.π.). Αυτά τα δίκτυα θεωρούνται «ημί-αξιόπιστα», λόγω του γεγονότος ότι επικοινωνούν με εξωτερικά δίκτυα.*
- *Δίκτυα Εσωτερικών Υπηρεσιών: Τα περισσότερα από τα δίκτυα και τα υποδίκτυα της ΕΕΤΤ π.χ. LANs, WANs κ.λ.π., τα οποία υποστηρίζουν την ομαλή εκτέλεση των επιχειρησιακών λειτουργιών και λειτουργούν στα πληροφοριακά συστήματα της ΕΕΤΤ ανήκουν σε αυτή την κατηγορία. Αυτά τα δίκτυα θεωρούνται «αξιόπιστα».*
- *Εσωτερικά Εμπιστευτικά Δίκτυα: Υπάρχουν εσωτερικά δίκτυα της ΕΕΤΤ τα οποία είναι απομονωμένα και υποστηρίζουν κρίσιμες λειτουργίες π.χ. υποδομές διαχείρισης ασφάλειας, υποδομές παρακολούθησης ασφάλειας κ.λ.π. Αυτά τα δίκτυα μπορούν να θεωρηθούν «αξιόπιστα».*

4.2.3 Ταξινόμηση των πληροφοριακών συστημάτων

Το επίπεδο ταξινόμησης το οποίο αποδίδεται σε ένα πληροφοριακό σύστημα προκύπτει αφού ληφθεί υπόψη το επίπεδο ταξινόμησης των εφαρμογών που φιλοξενούνται στο πληροφοριακό σύστημα και το επίπεδο ταξινόμησης του δικτύου με το οποίο είναι συνδεδεμένο ή επικοινωνεί το σύστημα.

Το τελικό επίπεδο ταξινόμησης που αποδίδεται στο σύστημα πρέπει πάντα να είναι υψηλότερο, αφού εξεταστούν όλες οι παράμετροι, που αναφέρονται παρακάτω.

Ως προς την εμπιστευτικότητα του πληροφοριακού συστήματος:

Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Κρίσιμο ως προς την εμπιστευτικότητα» αν ισχύει τουλάχιστον ένα από τα παρακάτω:

- *Τουλάχιστον μια από τις εφαρμογές που φιλοξενείται στο πληροφοριακό σύστημα χαρακτηρίζεται ως «Κρίσιμη ως προς την εμπιστευτικότητα» (σύμφωνα με τη μεθοδολογία που περιγράφεται σε προηγούμενη ενότητα) ή*
- *Η ταξινόμηση τουλάχιστον ενός εκ των πληροφοριακών συστημάτων με τα οποία συνδέεται άμεσα ή από τα οποία εξαρτάται το πληροφοριακό σύστημα είναι «Κρίσιμη ως προς την εμπιστευτικότητα».*

Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Ευαίσθητο ως προς την εμπιστευτικότητα», αν το υψηλότερο επίπεδο ταξινόμησης μεταξύ των παρακάτω είναι «ευαίσθητο ως προς την εμπιστευτικότητα»:

- *Το υψηλότερο επίπεδο ταξινόμησης των εφαρμογών που φιλοξενούνται στο πληροφοριακό σύστημα και*
- *Το υψηλότερο επίπεδο ταξινόμησης των πληροφοριακών συστημάτων με τα οποία αυτό το πληροφοριακό σύστημα συνδέεται άμεσα ή από τα οποία εξαρτάται.*

Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Μη-κρίσιμο ως προς την εμπιστευτικότητα» αν ισχύουν συνδυαστικά τα παρακάτω:

- *Όλες οι εφαρμογές που φιλοξενούνται στο πληροφοριακό σύστημα χαρακτηρίζονται ως «μη-κρίσιμες ως προς την εμπιστευτικότητα» (σύμφωνα με τη μεθοδολογία που περιγράφεται σε προηγούμενη ενότητα) και*
- *Η ταξινόμηση όλων των πληροφοριακών συστημάτων με τα οποία συνδέεται άμεσα ή από τα οποία εξαρτάται το πληροφοριακό σύστημα είναι «Μη-κρίσιμα ως προς 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

<u>Ως προς την ακεραιότητα του πληροφοριακού συστήματος:</u>

*Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Κρίσιμο ως προς την ακεραιότητα**»** αν ισχύει τουλάχιστον ένα από τα παρακάτω:*

- *Τουλάχιστον μια από τις εφαρμογές που φιλοξενείται στο πληροφοριακό σύστημα χαρακτηρίζεται ως «Κρίσιμη ως προς την ακεραιότητα**»** (σύμφωνα με τη μεθοδολογία που περιγράφεται σε προηγούμενη ενότητα) ή*
- *Η ταξινόμηση τουλάχιστον ενός εκ των πληροφοριακών συστημάτων με τα οποία συνδέεται άμεσα ή από τα οποία εξαρτάται το πληροφοριακό σύστημα είναι «Κρίσιμη ως προς την ακεραιότητα**».***

Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Ευαίσθητο ως προς την ακεραιότητα», αν το υψηλότερο επίπεδο ταξινόμησης μεταξύ των παρακάτω είναι «ευαίσθητο ως προς την ακεραιότητα»:

- *Το υψηλότερο επίπεδο ταξινόμησης των εφαρμογών που φιλοξενούνται στο πληροφοριακό σύστημα και*
- *Το υψηλότερο επίπεδο ταξινόμησης των πληροφοριακών συστημάτων με τα οποία αυτό το πληροφοριακό σύστημα συνδέεται άμεσα ή από τα οποία εξαρτάται.*

*Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Μη-κρίσιμο ως προς την ακεραιότητα**»** αν ισχύουν συνδυαστικά τα παρακάτω:*

- *Όλες οι εφαρμογές που φιλοξενούνται στο πληροφοριακό σύστημα χαρακτηρίζονται ως «μη-κρίσιμες ως προς την ακεραιότητα» (σύμφωνα με τη μεθοδολογία που περιγράφεται σε προηγούμενη ενότητα) και*
- *Η ταξινόμηση όλων των πληροφοριακών συστημάτων με τα οποία συνδέεται άμεσα ή από τα οποία εξαρτάται το πληροφοριακό σύστημα είναι «Μη-κρίσιμα ως προς την ακεραιότητα**».***

***<u>Ως προς την διαθεσιμότητα της εφαρμογής ως προς το χρόνο ανάκτησης</u>** <u>(RTO):</u>*

*Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Κρίσιμο ως προς το χρόνο ανάκτησης**»** αν ισχύει τουλάχιστον ένα από τα παρακάτω:*

- *Τουλάχιστον μια από τις εφαρμογές που φιλοξενείται στο πληροφοριακό σύστημα χαρακτηρίζεται ως «Κρίσιμη ως προς το χρόνο ανάκτησης**»** (σύμφωνα με τη μεθοδολογία που περιγράφεται σε προηγούμενη ενότητα) ή*
- *Η ταξινόμηση τουλάχιστον ενός εκ των πληροφοριακών συστημάτων με τα οποία συνδέεται άμεσα ή από τα οποία εξαρτάται το πληροφοριακό σύστημα είναι «Κρίσιμη ως προς το χρόνο ανάκτησης**».***

Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Ευαίσθητο ως προς το χρόνο ανάκτησης», αν το υψηλότερο επίπεδο ταξινόμησης μεταξύ των παρακάτω είναι «ευαίσθητο ως προς το χρόνο ανάκτησης»:

- *Το υψηλότερο επίπεδο ταξινόμησης των εφαρμογών που φιλοξενούνται στο πληροφοριακό σύστημα και*
- *Το υψηλότερο επίπεδο ταξινόμησης των πληροφοριακών συστημάτων με τα οποία αυτό το πληροφοριακό σύστημα συνδέεται άμεσα ή από τα οποία εξαρτάται.*

*Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Μη-κρίσιμο ως προς το χρόνο ανάκτησης**»** αν ισχύουν συνδυαστικά τα παρακάτω:*

- *Όλες οι εφαρμογές που φιλοξενούνται στο πληροφοριακό σύστημα χαρακτηρίζονται ως «μη-κρίσιμες ως προς το χρόνο ανάκτησης» (σύμφωνα με τη μεθοδολογία που περιγράφεται σε προηγούμενη ενότητα) και*
- *Η ταξινόμηση όλων των πληροφοριακών συστημάτων με τα οποία συνδέεται άμεσα ή από τα οποία εξαρτάται το πληροφοριακό σύστημα είναι «Μη-κρίσιμα ως προς το χρόνο ανάκτησης**».***

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

***Ως προς την διαθεσιμότητα της εφαρμογής ως προς το σημείο ανάκτησης** (RPO):*

*Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Κρίσιμο ως προς το σημείο ανάκτησης**»** αν ισχύει τουλάχιστον ένα από τα παρακάτω:*

- *Τουλάχιστον μια από τις εφαρμογές που φιλοξενείται στο πληροφοριακό σύστημα χαρακτηρίζεται ως «Κρίσιμη ως προς το σημείο ανάκτησης**»** (σύμφωνα με τη μεθοδολογία που περιγράφεται σε προηγούμενη ενότητα) ή*
- *Η ταξινόμηση τουλάχιστον ενός εκ των πληροφοριακών συστημάτων με τα οποία συνδέεται άμεσα ή από τα οποία εξαρτάται το πληροφοριακό σύστημα είναι «Κρίσιμη ως προς το σημείο ανάκτησης**».***

Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Ευαίσθητο ως προς το σημείο ανάκτησης», αν το υψηλότερο επίπεδο ταξινόμησης μεταξύ των παρακάτω είναι «ευαίσθητο ως προς το σημείο ανάκτησης»:

- *Το υψηλότερο επίπεδο ταξινόμησης των εφαρμογών που φιλοξενούνται στο πληροφοριακό σύστημα και*
- *Το υψηλότερο επίπεδο ταξινόμησης των πληροφοριακών συστημάτων με τα οποία αυτό το πληροφοριακό σύστημα συνδέεται άμεσα ή από τα οποία εξαρτάται.*

*Ένα πληροφοριακό σύστημα χαρακτηρίζεται ως «Μη-κρίσιμο ως προς το σημείο ανάκτησης**»** αν ισχύουν συνδυαστικά τα παρακάτω:*

- *Όλες οι εφαρμογές που φιλοξενούνται στο πληροφοριακό σύστημα χαρακτηρίζονται ως «μη-κρίσιμες ως προς το σημείο ανάκτησης» (σύμφωνα με τη μεθοδολογία που περιγράφεται σε προηγούμενη ενότητα) και*
- *Η ταξινόμηση όλων των πληροφοριακών συστημάτων με τα οποία συνδέεται άμεσα ή από τα οποία εξαρτάται το πληροφοριακό σύστημα είναι «Μη-κρίσιμα ως προς το σημείο ανάκτησης**»**.*

Σύμφωνα με τα παραπάνω οριζόμενα στην παρούσα πολιτική, η ΕΕΤΤ προσδιορίζει για κάθε πληροφοριακό σύστημα τα τρία επίπεδα κρισιμότητάς του, δηλαδή ως προς την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητά του και στη συνέχεια βάσει αυτών καθορίζει και τα μέτρα ασφαλείας που πρέπει να λαμβάνει αντίστοιχα για την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα του συστήματος. Όσο πιο κρίσιμο είναι ένα σύστημα, τόσο πιο αυστηρά μέτρα ασφάλειας απαιτούνται για την προστασία του.

4.3 Πρόσθετα θέματα σχετικά με την ταξινόμηση των πληροφοριακών πόρων

4.3.1 Περιοδικός έλεγχος του επιπέδου ταξινόμησης

Το επίπεδο ταξινόμησης των πληροφοριακών πόρων πρέπει να ελέγχεται τακτικά από τους αρμόδιους ιδιοκτήτες των πληροφοριακών πόρων και να αναθεωρείται όταν απαιτείται.

4.3.2 Σήμανση για την ταξινόμηση των πληροφοριακών πόρων

Όλοι οι κρίσιμοι / ευαίσθητοι πληροφοριακοί πόροι, όπου είναι εφαρμόσιμο και εφικτό, πρέπει να φέρουν ευδιάκριτη σήμανση (π.χ. ετικέτα ταξινόμησης), από τη δημιουργία τους μέχρι την απόσυρσή τους ή την αναθεώρηση της ταξινόμησής τους, δηλώνοντας το επίπεδο ταξινόμησής τους και κατά συνέπεια την αξία και την κρισιμότητά τους. Σήμανση ταξινόμησης (όπου είναι εφικτό) πρέπει να χρησιμοποιείται είτε οι πληροφορίες είναι σε έγχαρτη φυσική είτε σε ηλεκτρονική μορφή και αναλόγως να φυλάσσονται σε ασφαλή τοποθεσία. Οι πληροφορίες που δεν φέρουν σήμανση θεωρούνται «ΕΣΩΤΕΡΙΚΗΣ ΧΡΗΣΗΣ» ως προς την αρχή της εμπιστευτικότητας.

Το Σύστημα Ηλεκτρονικής Διαχείρισης Εγγράφων της ΕΕΤΤ (ΣΗΔΕ) διαχειρίζεται και παρακολουθεί εντελώς χωριστά, με διακριτό πρωτόκολλο, τα εμπιστευτικά, τα εσωτερικής χρήσης και τα λοιπά έγγραφα. Επομένως, μέσα στο ΣΗΔΕ τα έγγραφα είναι διαχωρισμένα σύμφωνα με την παραπάνω ταξινόμηση. Παράλληλα, οι πληροφορίες εσωτερικής χρήσης που απευθύνονται σε όλο το προσωπικό διατηρούνται αναρτημένες στη Γνωσιακή Πύλη "Εστία". Ενώ οι δημόσιες πληροφορίες αναρτώνται στο διαδικτυακό τόπο της ΕΕΤΤ (www.eett.gr), σύμφωνα με τη σχετική εγκριτική διαδικασία της ΕΕΤΤ, προκειμένου να είναι προσβάσιμες από το ευρύ κοινό.

4.3.3 Λήψη μέτρων ασφαλείας για τους πληροφοριακούς πόρους ανάλογα με το επίπεδο ταξινόμησης

Η διαδικασία ταξινόμησης πληροφοριακών πόρων ακολουθείται για όλους τους πληροφοριακούς πόρους 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

Τα μέτρα ασφάλειας που απαιτούνται και λαμβάνονται ανά πληροφοριακό πόρο εξαρτώνται από το επίπεδο ταξινόμησής του. Έτσι, άπαξ και ταξινομηθούν, οι πληροφοριακοί πόροι προστατεύονται σύμφωνα με την ταξινόμησή τους, καθ' όλη τη διάρκεια της ζωής τους, από τη δημιουργία τους μέχρι την απόσυρσή τους ή μέχρι να αναθεωρηθεί η ταξινόμησή τους (στην περίπτωση αλλαγής συνθηκών).

Το κόστος που δαπανάται για την ασφάλεια του κάθε πληροφοριακού πόρου πρέπει να είναι ανάλογο με την υπηρεσιακή αξία του, δηλαδή ανάλογο με το επίπεδο της κρισιμότητάς του. Όταν απαιτείται, οι πληροφοριακοί πόροι υποστηρίζονται από συστήματα ασφάλειας που έχουν σχεδιαστεί να προστατεύουν την εμπιστευτικότητα, ακεραιότητα ή/και διαθεσιμότητά τους και παρέχουν τους κατάλληλους τρόπους για την ανίχνευση περιστατικών ασφαλείας και την ανάκτηση των πληροφοριών όταν απαιτείται.

4.4 Ταξινόμηση χρηστών των πληροφοριακών πόρων

Προκειμένου να διασφαλίσει την ασφαλή πρόσβαση στους πληροφοριακούς πόρους της, η ΕΕΤΤ ταξινομεί πέρα από τους πληροφοριακούς πόρους και τους χρήστες που έχουν ή εν δυνάμει θα μπορούσαν να έχουν πρόσβαση σε αυτούς.

Με στόχο να αξιολογηθεί και να αποδοθεί το επίπεδο ταξινόμησης στους χρήστες, τρεις βασικές παράμετροι εκτιμώνται:

- *Το επίπεδο εμπιστοσύνης του χρήστη*
- *Το καθορισμένο επίπεδο πρόσβασης*
- *Το καθορισμένο είδος πρόσβασης*

4.4.1 Επίπεδο εμπιστοσύνης

Η πρόσβαση του χρήστη πρέπει καταρχήν να ελέγχεται σύμφωνα με το «Επίπεδο Εμπιστοσύνης». Το επίπεδο εμπιστοσύνης εξαρτάται από τη σχέση κάθε χρήστη με την ΕΕΤΤ.

Οι παρακάτω βασικές κατηγορίες χρηστών προσδιορίζονται με βάση το επίπεδο εμπιστοσύνης:

- *Αξιόπιστοι: Οι χρήστες που είναι είτε μόνιμοι είτε προσωρινοί εργαζόμενοι της ΕΕΤΤ.*
- *Ημι-αξιόπιστοι: Γνωστοί στην ΕΕΤΤ χρήστες (μη εργαζόμενοι στην ΕΕΤΤ) των οποίων η πρόσβαση μπορεί να ελεγχθεί είτε σε επίπεδο επιχείρησης που ανήκουν είτε σε προσωπικό επίπεδο. Η πρόσβαση στα πληροφοριακά συστήματα της ΕΕΤΤ παρέχεται με βάση κανονισμούς, συμβάσεις, κτλ., όπως ισχύουν σε κάθε περίπτωση.*

  Οι παρακάτω ενδεικτικές κατηγορίες χρηστών εμπίπτουν σε αυτή την κατηγορία:

  - *Πάροχοι: Φυσικά πρόσωπα ή εταιρείες οι οποίοι έχουν πρόσβαση στις υπηρεσίες / συστήματα της ΕΕΤΤ βάσει κανονισμών.*
  - *Τρίτοι: Κάθε τρίτη εταιρεία (π.χ. συνεργαζόμενες εταιρείες, προμηθευτές, εξωτερικοί σύμβουλοι, υπεργολάβοι και πάροχοι άλλων υπηρεσιών κ.λ.π.), η στενή συνεργασία με την οποία είναι ζωτικής σημασίας, λόγω των παρεχόμενων υπηρεσιών με σκοπό την υποστήριξη της υπηρεσιακής λειτουργίας της ΕΕΤΤ.*
- *Μη-αξιόπιστοι: Άγνωστοι χρήστες, στους οποίους επιτρέπεται περιορισμένη πρόσβαση στους πληροφοριακούς πόρους της ΕΕΤΤ.*

Αναλόγως του παραπάνω επιπέδου εμπιστοσύνης των χρηστών αποδίδονται καταρχήν και τα δικαιώματα πρόσβασης σε πληροφορίες, βάσει του επιπέδου ταξινόμησής τους, όπως παρατίθεται στον κάτωθι πίνακα.

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

Προσβασιμότητα χρηστών σύμφωνα με το επίπεδο ταξινόμησης πληροφοριών			
Χρήστες	**Άκρως Απόρρητες, Απόρρητες, Εμπιστευτικές (με εξουσιοδότηση)**	**Εσωτερικής χρήσης (με εξουσιοδότηση)**	**Δημόσιες**
Αξιόπιστοι	☑	☑	☑
Ημι-αξιόπιστοι	☒	☑	☑
Μη-αξιόπιστοι	☒	☒	☑

Επομένως, σύμφωνα με τον πίνακα:

- *Οι χρήστες που, εφόσον εξουσιοδοτηθούν, μπορούν να έχουν πρόσβαση σε άκρως απόρρητες, απόρρητες ή εμπιστευτικές πληροφορίες ανήκουν υποχρεωτικά και μόνο στους Αξιόπιστους χρήστες. Αντιθέτως, οι Ημι-αξιόπιστοι και οι Μη-αξιόπιστοι χρήστες δεν επιτρέπεται να έχουν πρόσβαση σε αυτές τις πληροφορίες.*
- *Οι Μη-αξιόπιστοι χρήστες δεν επιτρέπεται να έχουν πρόσβαση στις πληροφορίες εσωτερικής χρήσης. Οι Αξιόπιστοι και οι Ημι-αξιόπιστοι εφόσον εξουσιοδοτηθούν μπορούν να έχουν πρόσβαση σε αυτές.*
- *Μόνο στις δημόσιες πληροφορίες μπορούν να έχουν πρόσβαση όλοι οι χρήστες, ανεξάρτητα με το επίπεδο εμπιστοσύνης τους.*

4.4.2 Επίπεδο πρόσβασης

Η πρόσβαση του χρήστη ελέγχεται σύμφωνα με το «Επίπεδο Πρόσβασης». Το επίπεδο πρόσβασης εξαρτάται από τα δικαιώματα πρόσβασης που παρέχονται στους χρήστες σε κάθε πληροφοριακό σύστημα:

- *Απλή πρόσβαση: Οι χρήστες με δικαιώματα απλής πρόσβασης στα πληροφοριακά συστήματα / εφαρμογές της ΕΕΤΤ.*
- *Προνομιακή πρόσβαση: Οι χρήστες με αναβαθμισμένα δικαιώματα χρήστη σχετικά με τα πληροφοριακά συστήματα / εφαρμογές της ΕΕΤΤ. Αυτοί οι χρήστες είναι δυνατό να εκτελούν δραστηριότητες ανάπτυξης, διαχείρισης ή παρακολούθησης δραστηριοτήτων στα πληροφοριακά συστήματα της ΕΕΤΤ. Χρήστες που δεν έχουν τέτοιες αρμοδιότητες (ανάπτυξης, διαχείρισης ή παρακολούθησης των συστημάτων / εφαρμογών), δεν επιτρέπεται να έχουν προνομιακή πρόσβαση.*

Λεπτομέρειες για την απόδοση δικαιωμάτων πρόσβασης στους χρήστες βάσει των αρμοδιοτήτων τους, αναλύονται στις σχετικές πολιτικές της ΕΕΤΤ.

4.4.3 Είδος πρόσβασης

Η πρόσβαση των χρηστών πρέπει να ελέγχεται, επίσης, σύμφωνα με το «Είδος Πρόσβασης». Το είδος της πρόσβασης εξαρτάται από την κρισιμότητα των πληροφοριακών συστημάτων σε συνδυασμό με τη μέθοδο πρόσβασης.

- *Εσωτερική πρόσβαση στα πληροφοριακά συστήματα της ΕΕΤΤ: Η πρόσβαση των χρηστών στα πληροφοριακά συστήματα της ΕΕΤΤ με χρήση του δικτύου της.*
- *Πρόσβαση στα πληροφοριακά συστήματα της ΕΕΤΤ από απόσταση: Η πρόσβαση χρηστών στα πληροφοριακά συστήματα της ΕΕΤΤ με χρήση εξωτερικού δικτύου.*
- *Πρόσβαση σε συστήματα τρίτων μέσω της υποδομής της ΕΕΤΤ: Η πρόσβαση του χρήστη σε πληροφοριακά συστήματα τρίτων με χρήση της υποδομής 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

5 Γενικά θέματα διαχείρισης των πληροφοριακών πόρων

Οι πληροφοριακοί πόροι χρησιμοποιούνται ευρέως στην ΕΕΤΤ και είναι κρίσιμοι για την καθημερινή λειτουργία της. Η επένδυση σε αυτούς περιλαμβάνει εκτός από το κόστος προμήθειας και εγκατάστασης, λειτουργικά κόστη, όπως το κόστος συντήρησης, υποστήριξης, εκπαίδευσης και προστασίας τους. Η ασφαλής διαχείριση των πληροφοριακών πόρων διενεργείται μόνο από εξειδικευμένο και εκπαιδευμένο προσωπικό. Ειδικότερα, για την ασφαλή διαχείριση των πληροφοριών περισσότερες λεπτομέρειες αναλύονται στην Πολιτική Διατήρησης Πληροφοριών.

5.1 Απόκτηση πληροφοριακών πόρων και ένταξη σε λειτουργία

Όλοι οι πληροφοριακοί πόροι αποκτώνται στο απαιτούμενο πλήθος (π.χ. πλήθος αδειών χρήσης) από την ΕΕΤΤ, σύμφωνα με τις υπάρχουσες διαδικασίες προμηθειών που καθορίζονται από το σχετικό νομοθετικό πλαίσιο.

Οι εισερχόμενοι και καινούργιοι πληροφοριακοί πόροι επισημαίνονται και καταγράφονται σύμφωνα με το σύστημα κωδικοποίησης που χρησιμοποιείται.

Πριν την εγκατάσταση και θέση σε λειτουργία κάθε πληροφοριακού πόρου, ορίζεται ένας ιδιοκτήτης, όπως έχει ήδη ειπωθεί. Ο ιδιοκτήτης παραχωρεί τα δικαιώματα πρόσβασης σχετικά με τον πληροφοριακό πόρο, τον καταγράφει στο μητρώο πληροφοριακών πόρων και τον ταξινομεί.

Η εγκατάσταση και ένταξη σε λειτουργία των πληροφοριακών πόρων γίνεται με βάση τις πρότυπες διαδικασίες της ΕΕΤΤ.

5.2 Χρήση πληροφοριακών πόρων

Ακολουθείται ορθή και λελογισμένη χρήση των πληροφοριακών πόρων, δηλαδή χρήση που είναι σύμφωνη με τους υπηρεσιακούς και διοικητικούς στόχους της ΕΕΤΤ αλλά και με τους συγκεκριμένους στόχους ενός έργου ή μιας εργασίας για τους οποίους έχει εξουσιοδοτηθεί η συγκεκριμένη χρήση του πόρου. Οποιαδήποτε άλλου είδους χρήση θεωρείται μη αποδεκτή. Επίσης, η σκόπιμη σπατάλη των πόρων είναι μη αποδεκτή ενέργεια.
Οι χρήστες των πληροφοριακών πόρων είναι υπεύθυνοι:

- *Να συμμορφώνονται με τις διαδικασίες ασφαλείας που χρησιμοποιούνται ή επιβάλλονται από τους ιδιοκτήτες*
- *Να χρησιμοποιούν και να προστατεύουν τους πληροφοριακούς πόρους, όπως θα προστάτευαν ένα έγγραφο με το ίδιο επίπεδο ταξινόμησης*

Περισσότερες λεπτομέρειες για την ασφαλή χρήση των πληροφοριακών πόρων της ΕΕΤΤ αναλύονται στην Πολιτική Ασφάλειας Τελικού Χρήστη.

5.3 Παρακολούθηση της μεταφοράς πληροφοριακών πόρων

Πριν μετακινηθεί ή μεταφερθεί εντός ή εκτός των εγκαταστάσεων της ΕΕΤΤ ένας πληροφοριακός πόρος, απαιτείται εξουσιοδότηση από τον ιδιοκτήτη του.

Κάθε μετακίνηση ή μεταφορά ενός πληροφοριακού πόρου πρέπει να καταγραφεί και τα αρχεία που δημιουργούνται πρέπει να τηρηθούν για να υπάρχει απόδειξη της αποτελεσματικής παρακολούθησης των πληροφοριακών πόρων στις εγκαταστάσεις της ΕΕΤΤ και για να ικανοποιούνται οι απαιτήσεις ελέγχου.

Σε κάθε περίπτωση το μητρώο πληροφοριακών πόρων ενημερώνεται σχετικά.

Εξαιρούνται των ανωτέρω υποχρεώσεων, οι φορητοί υπολογιστές και φορητές συσκευές για τα οποία παρέχεται η αντίστοιχη εξουσιοδότηση φορητότητας στον χρήστη με την παράδοσή τους σε αυτόν.

5.4 Συντήρηση πληροφοριακών πόρων

Οι πληροφοριακοί πόροι συντηρούνται με κατάλληλο τρόπο, ώστε να εξασφαλίζεται η διαρκής διαθεσιμότητα και ακεραιότητά τους.

5.5 Αποθήκευση πληροφοριακών πόρων και περιβάλλον προστασίας

Οι πληροφοριακοί πόροι αποθηκεύονται με ασφάλεια σε ελεγχόμενες περιοχές και συγκεκριμένες περιβαλλοντικές συνθήκες, σύμφωνα με το επίπεδο ταξινόμησής τους.

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

Οι απαιτήσεις χωρητικότητας πληροφοριακών πόρων προσδιορίζονται, παρακολουθούνται, αναλύονται, ρυθμίζονται, εφαρμόζονται και τεκμηριώνονται ώστε να εξασφαλίζεται ότι η υπάρχουσα χωρητικότητα ανταποκρίνεται στις τρέχουσες και στις εκτιμώμενες μελλοντικές υπηρεσιακές απαιτήσεις.

Οι απαιτήσεις διαθεσιμότητας των πληροφοριακών πόρων πρέπει να προσδιορίζονται, μετριούνται, αναλύονται, προγραμματίζονται και να λαμβάνονται οι αναγκαίες ενέργειες προκειμένου να εξασφαλίζεται ότι οι πληροφοριακοί πόροι έχουν τα επίπεδα διαθεσιμότητας που απαιτούνται από την ΕΕΤΤ και ότι τα σχετικά σχέδια επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές ενημερώνονται ανάλογα.

5.6 Πληροφοριακοί πόροι και έλεγχοι

Οι πληροφοριακοί πόροι της ΕΕΤΤ πρέπει να ελέγχονται ως προς την δημιουργία, την εξουσιοδοτημένη χρήση, τη λειτουργία και την καταστροφή τους.

Οι έλεγχοι στους πληροφοριακούς πόρους πρέπει να γίνονται σε τακτική βάση και να βασίζονται σε μεθοδολογία δειγματοληψίας.

Οι διεξαγόμενοι έλεγχοι πρέπει να εξασφαλίζουν ότι οι πληροφοριακοί πόροι που βρίσκονται εντός του πεδίου του ελέγχου είναι ακόμα σε λειτουργία ή αποθηκευμένοι σε χώρους που βρίσκονται σε συγκεκριμένες τοποθεσίες και, όπου είναι εφικτό, φέρουν την κατάλληλη σήμανση σχετικά με το επίπεδο ταξινόμησης του πληροφοριακού πόρου.

Η απόσυρση των πληροφοριακών πόρων διενεργείται σύμφωνα με τις εκάστοτε πολιτικές της ΕΕΤΤ.

5.7 Διαχείριση περιστατικών παραβίασης της ασφάλειας των πληροφοριακών πόρων

Όταν κάποιο μέλος του προσωπικού της ΕΕΤΤ παρατηρήσει κάποια παραβίαση της ασφάλειας πληροφοριακού πόρου, πρέπει να την αναφέρει άμεσα στην Διεύθυνση Ψηφιακής Διακυβέρνησης.

Η κρισιμότητα ενός περιστατικού, μεταξύ άλλων, καθορίζεται από την κρισιμότητα των πληροφοριών και των συστημάτων ή εφαρμογών που επηρεάστηκαν ή μπορεί να επηρεαστούν και τη σοβαρότητα του άμεσου ή έμμεσου αντικτύπου του συμβάντος λαμβάνοντας υπόψη την αλληλεπίδραση συστημάτων και εφαρμογών.

Όταν απαιτείται από τη νομοθεσία, η ΕΕΤΤ αναφέρει περιστατικά παραβίασης της ασφάλειας στις αρμόδιες αρχές.

Λεπτομέρειες για την διαχείριση των περιστατικών ασφαλείας, αναλύονται στην Πολιτική Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών 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

ΠΑΡΑΡΤΗΜΑ Α: Υπόδειγμα πίνακα για την εκτίμηση της κρισιμότητας μιας εφαρμογής βάσει των πληροφοριών που περιλαμβάνει

Σύνολο Δεδομένων	***Κωδ. Συνόλου Δεδομένων***	***Ταξινόμηση ως προς την Εμπιστευτικότητα***	***Ταξινόμηση ως προς την Ακεραιότητα***	***Ταξινόμηση ως προς το χρόνο ανάκτησης***	***Ταξινόμηση ως προς το σημείο ανάκτησης***	***Κρισιμότητα Συνόλου Δεδομένων***	***Ένδειξη Προσωπικών Δεδομένων***	***Ένδειξη Ανοικτών Δεδομένων***	***Παρατηρήσεις***
Σύνολο Α		*Άκρως απόρρητο ή απόρρητο ή εμπιστευτικό ή εσωτερικής χρήσης ή δημόσιο*	*Υψηλή ή Μεσαία ή Χαμηλή*	*Πολύ Υψηλή ή Υψηλή ή Μεσαία ή Χαμηλή ή Πολύ χαμηλή*	*Πολύ Υψηλή ή Υψηλή ή Μεσαία ή Χαμηλή ή Πολύ χαμηλή*	*Κρίσιμη ή Ευαίσθητη ή Μη Κρίσιμη*	*Ναι ή Όχι*	*Ναι ή Όχι*	
Σύνολο Β		>>	>>	>>	>>	>>			
Σύνολο Γ		>>	>>	>>	>>	>>			
Κτλ.		>>	>>	>>	>>	>>			
Εφαρμογή		***Κρισιμότητα εφαρμογής ως προς την Εμπιστευτικότητα*** *(Κρίσιμη ή Ευαίσθητη ή Μη Κρίσιμη)*	***Κρισιμότητα εφαρμογής ως προς την Ακεραιότητα*** *(Κρίσιμη ή Ευαίσθητη ή Μη Κρίσιμη)*	***Κρισιμότητα εφαρμογής ως προς το χρόνο ανάκτησης*** *(Κρίσιμη ή Ευαίσθητη ή Μη Κρίσιμη)*	***Κρισιμότητα εφαρμογής ως προς το σημείο ανάκτησης*** *(Κρίσιμη ή Ευαίσθητη ή Μη Κρίσιμη)*				

Σύμφωνα με τον παραπάνω πίνακα, προκειμένου να εκτιμηθεί η κρισιμότητα μιας εφαρμογής, πρώτα ταξινομούνται όλα τα διαφορετικά είδη πληροφορίας (σύνολα δεδομένων) που αυτή αποθηκεύει και επεξεργάζεται ως προς την εμπιστευτικότητα, ακεραιότητα, χρόνο ανάκτησης και σημείο ανάκτησης, σύμφωνα με το σύστημα ταξινόμησης που αναλύεται στις ενότητες 4.1.1, 4.1.2, 4.1.3, αντίστοιχα. Στη συνέχεια, βάσει αυτών εκτιμάται η κρισιμότητα της εφαρμογής, όπως περιγράφεται στην ενότητα 4.2.1. Παράλληλα, η κρισιμότητα του κάθε συνόλου δεδομένων εξάγεται σύμφωνα με τους κανόνες που περιγράφονται στην ενότητα 4.1.4, ενώ επιπλέον ενδείξεις για τα προσωπικά δεδομένα ή τα ανοικτά δεδομένα αποδίδονται βάσει των οριζόμενων στην ενότητα 4.1.5.»

2. **Εντέλλεται** την κοινοποίηση της παρούσας Απόφασης στο προσωπικό της ΕΕΤΤ μέσω ανάρτησής της στη Γνωσιακή Πύλη (portal) και αποστολής της με μήνυμα ηλεκτρονικού ταχυδρομείου.
3. **Ορίζει** ότι η «Πολιτική Διαχείρισης Πληροφοριακών Πόρων» συνδέεται άρρηκτα με τις υπό στοιχείο 4΄, 5΄, 6΄, 7΄, 8΄ ως άνω πολιτικές ασφαλείας της ΕΕΤΤ και πρέπει να εφαρμόζεται υποχρεωτικά και απαρέγκλιτα από το προσωπικό της.
4. **Εξουσιοδοτεί** το 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 Διαχείρισης Πληροφοριακών Πόρων»*.
   - Τροποποιεί την *«Πολιτική Διαχείρισης Πληροφοριακών Πόρων»*, όποτε αυτό απαιτείται.

Ο ΠΡΟΕΔΡΟΣ

ΚΑΘΗΓΗΤΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ ΜΑΣΣΕΛΟΣ

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