ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

Μαρούσι, 17-11-2025

ΑΠ 1174/14

ΑΠΟΦΑΣΗ

Έγκριση της «Πολιτικής Διαχείρισης Λογικής Πρόσβασης»

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 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),

1.9 του Ν. 5160/2024 «*Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του Κανονισμού (ΕΕ) 910/2014 και της Οδηγίας (ΕΕ) 2018/1972, και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS 2) και άλλες διατάξεις*» (Α΄ 195),

1.10 της ΚΥΑ υπ' αρ. 1689/30-4-2025 «*Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων*» (ΦΕΚ 2186/Β΄/6-5-2025),

1.11 της Υ.Α. 1899/27-06-2025 *«Καθορισμός προσόντων, καθηκόντων, ασυμβιβάστων και υποχρεώσεων των Υπεύθυνων Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών»* (ΦΕΚ 4250/Β΄/05-08-2025),

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, όπως ισχύει μετά την αναθεώρησή της με την ΑΠ 1157/33/16-6-2025 Απόφαση της ΕΕΤΤ «*Έγκριση της εφαρμογής της αναθεωρημένης «Πολιτικής Ασφαλείας» της ΕΕΤΤ*»,
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 1046/15/10-10-2022 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Τηλεργασίας και Φορητών Συσκευών"*»,
7. Την ΑΠ 1048/13/24-10-2022 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Συμβάντων Ασφαλείας Πληροφοριών"*»,
8. Την ΑΠ 1050/26/07-11-2022 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Φυσικής και Περιβαλλοντικής Ασφάλειας"*»,
9. Την ΑΠ 1089/32/30-10-2023 Απόφαση της ΕΕΤΤ «*Έγκριση της «Πολιτικής Διατήρησης Πληροφοριών»*»,
10. Την ΑΠ 1115/11/10-06-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Πληροφοριακών Πόρων"»*,
11. Την ΑΠ 1125/17/16-09-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Αλλαγών στα Υπολογιστικά Συστήματα"*»,
12. Την ΑΠ 1128/24/07-10-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Προμήθειας και Ανάπτυξης Συστημάτων"*»,
13. Την ΑΠ 1138/24/23-12-2024 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Διαχείρισης Τρίτων Μερών"*»,

14. Την ΑΠ 1161/13/21-07-2025 Απόφαση της ΕΕΤΤ *«Έγκριση της "Πολιτικής Διενέργειας Ελέγχων Ασφάλειας Πληροφοριών"»*,
15. Την ΑΠ 1168/14/29-09-2025 Απόφαση της ΕΕΤΤ «*Έγκριση της "Πολιτικής Παρακολούθησης Ασφάλειας Συστημάτων"*»,
16. Την ΑΠ 1109/13/15-4-2024 Απόφαση της ΕΕΤΤ «*Επικύρωση του Εγχειριδίου Διαδικασιών της ΕΕΤΤ*»,
17. Την ΑΠ 1142/21/10-02-2025 Απόφαση της ΕΕΤΤ «*Προσθήκη νέας οργανικής μονάδας και τροποποίηση της Διεύθυνσης Τηλεπικοινωνιών του Οργανισμού της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων όπως αυτός έχει εγκριθεί με την υπό στοιχεία ΑΠ ΕΕΤΤ 996/08/22.6.2021 απόφαση*» (ΦΕΚ 1280/Β΄/2025),
18. Το γεγονός ότι από τις διατάξεις της παρούσας Απόφασης δεν προκαλείται δαπάνη σε βάρος του κρατικού προϋπολογισμού ούτε του προϋπολογισμού της ΕΕΤΤ,
19. Την Εισήγηση αριθ. 38746/Φ600/11-11-2025 της αρμόδιας Υπηρεσίας της ΕΕΤΤ,

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

Επειδή :

1. Η διαχείριση της πρόσβασης στους πληροφοριακούς πόρους ενός οργανισμού είναι θεμελιώδης διεργασία για τη μείωση των κινδύνων που απειλούν την ασφάλεια της πληροφορίας στον οργανισμό.
2. Η υπό στοιχείο (4.) ως άνω Πολιτική Ασφαλείας της ΕΕΤΤ περιέγραψε, μόνο με συνοπτικό τρόπο, τις αρχές και τα πρότυπα που διέπουν τον έλεγχο της φυσικής και λογικής πρόσβασης στα πληροφοριακά συστήματα της ΕΕΤΤ.

3. Στη συνέχεια, τα μέτρα φυσικής πρόσβασης για την προστασία από τη μη εξουσιοδοτημένη φυσική πρόσβαση στις εγκαταστάσεις, στα computer rooms και στους πληροφοριακούς πόρους της ΕΕΤΤ εξειδικεύτηκαν στην υπό στοιχείο (8.) ως άνω «Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας».
4. Κρίνεται σκόπιμη η σύνταξη και γνωστοποίηση στο προσωπικό της ΕΕΤΤ μιας πολιτικής η οποία θα εξειδικεύει τα μέτρα τα οποία λαμβάνει η ΕΕΤΤ και τους κανόνες που θέτει, προκειμένου να επιτρέπει ή να απαγορεύει τη λογική πρόσβαση (δηλαδή την πρόσβαση μέσω υπολογιστή) στους πληροφοριακούς πόρους της, διασφαλίζοντας ότι μόνο τα πρόσωπα και τα συστήματα που απαιτείται και διαθέτουν την κατάλληλη εξουσιοδότηση έχουν πραγματικά τη δυνατότητα προσπέλασης και επέμβασης σε αυτούς.
5. Η πολιτική αυτή θα πρέπει να αφορά τόσο τους απλούς όσο και τους προνομιακούς χρήστες και να παρέχει τις δυνατότητες αναγνώρισης και ταυτοποίησης των χρηστών ότι είναι πράγματι αυτοί που ισχυρίζονται, καθώς και απόδοσης διαφορετικών δικαιωμάτων πρόσβασης και κατάλληλων επιπέδων εξουσιοδότησης σύμφωνα με το ρόλο και τις αρμοδιότητές τους μέσα στην ΕΕΤΤ.

Αποφασίζει :

1. **Εγκρίνει** *την «Πολιτική Διαχείρισης Λογικής Πρόσβασης», η οποία έχει ως εξής:*

« ***Πολιτική Διαχείρισης Λογικής Πρόσβασης***

Έκδοση: 1η

Τελευταία Ημερομηνία Ενημέρωσης: Νοέμβριος 2025

1 Σκοπός και πεδίο εφαρμογής

Σκοπός της παρούσας πολιτικής είναι ο καθορισμός ενός ενιαίου συνόλου αρχών οι οποίες θα διέπουν τη διαχείριση της λογικής πρόσβασης στα πληροφοριακά συστήματα της ΕΕΤΤ με βάση τις αρμοδιότητές της και τα πρότυπα ασφάλειας. Αφορά το προσωπικό της ΕΕΤΤ και το προσωπικό τρίτων μερών, όπως προμηθευτών και παρόχων υπηρεσιών τεχνολογιών πληροφορικής και επικοινωνιών που έχουν λογική πρόσβαση στα συστήματα της ΕΕΤΤ.

Η παρούσα πολιτική δεν ασχολείται με θέματα φυσικής πρόσβασης, τα οποία αποτελούν αντικείμενο της Πολιτικής Φυσικής και Περιβαλλοντικής Ασφάλειας.

2 Γενικά θέματα

2.1 Βασικές αρχές ελέγχου πρόσβασης

Οι έλεγχοι λογικής πρόσβασης (οργανωτικοί, τεχνικοί ή διοικητικοί/επιχειρησιακοί) που διέπουν τον τρόπο με τον οποίο οι χρήστες και τα πληροφοριακά συστήματα επικοινωνούν με άλλα πληροφοριακά συστήματα ή/και χρήστες, πρέπει να έχουν τα παρακάτω χαρακτηριστικά:

- *Να είναι σύμφωνοι με τις απαιτήσεις ασφαλείας των επιμέρους πληροφοριακών συστημάτων της ΕΕΤΤ.*
- *Να είναι σύμφωνοι με τις αρχές της «ανάγκης γνώσης» (need to know), των «ελαχίστων προνομίων» (least privilige) και της «ανάγκης διατήρησης» (need to retain) (βλ. παρακάτω τις ενότητες 2.6, 2.7 και 2.8).*
- *Να καθορίζονται βάσει τυπικών προφίλ χρηστών για τους κοινούς ρόλους εργασίας της ΕΕΤΤ.*
- *Να καθορίζονται και να επιλέγονται βάσει των αποτελεσμάτων της ανάλυσης κινδύνου.*
- *Να είναι σύμφωνοι με τις ισχύουσες νομικές και κανονιστικές απαιτήσεις.*
- *Να είναι σύμφωνοι με τις πολιτικές και τους κανονισμούς της ΕΕΤΤ.*
- *Να υποστηρίζονται από τις κατάλληλες διαδικασίες διαχείρισης προσβάσεων.*
- *Να είναι σχεδιασμένοι και υλοποιημένοι με τέτοιο τρόπο, ώστε να εξασφαλίζεται το κατάλληλο επίπεδο διαχωρισμού των καθηκόντων (separation of duties). Σε περιπτώσεις που αυτό δεν μπορεί να εφαρμοστεί, θα πρέπει να εφαρμόζονται αντισταθμιστικοί έλεγχοι για το μετριασμό των κινδύνων.*
- *Να είναι εφαρμόσιμοι για όλες τις συσκευές δικτύου, τις συσκευές ασφάλειας, τις βάσεις δεδομένων, τα λειτουργικά συστήματα και τις εφαρμογές της ΕΕΤΤ.*

2.2 Απαιτήσεις για τους μηχανισμούς ελέγχου πρόσβασης

Οι έλεγχοι πρόσβασης πρέπει να εξασφαλίζουν επαρκή αναγνώριση, έλεγχο ταυτότητας και εξουσιοδότηση των χρηστών που έχουν πρόσβαση στα πληροφοριακά συστήματα.

2.3 Μητρώο χρηστών και προσβάσεων

Η ΕΕΤΤ διαθέτει εφαρμογή διαχείρισης προσβάσεων, η οποία περιλαμβάνει το μητρώο προσβάσεων των χρηστών της, όπου τηρείται η πληροφορία ποιος εργαζόμενος έχει λογική πρόσβαση σε ποιο πληροφοριακό πόρο (όπως στο fileserver, στα email groups, στις κυριότερες εφαρμογές) και με τι δικαιώματα. Η εφαρμογή αυτή ενημερώνεται αυτόματα με τις αλλαγές προσβάσεων σε εφαρμογές και κοινόχρηστους φακέλους σε ημερήσια βάση (βλ. τη διαδικασία διαχείρισης προσβάσεων στο Εγχειρίδιο Διαδικασιών της ΕΕΤΤ) και παρέχει τη δυνατότητα αναζήτησης των δικαιωμάτων πρόσβασης στα κεντρικά συστήματα και τις κυριότερες εφαρμογές. Απευθύνεται κυρίως στους προϊσταμένους των οργανικών μονάδων που, ως ιδιοκτήτες πληροφοριών (information owners), έχουν την ευθύνη του ελέγχου της ορθής παροχής προσβάσεων στα πληροφοριακά συστήματα και τους πόρους της ΕΕΤΤ.

Οι ιδιοκτήτες των πληροφοριών συμβουλεύονται την εφαρμογή διαχείρισης προσβάσεων για τους πληροφοριακούς πόρους που περιλαμβάνονται σε αυτήν. Για τους λοιπούς πληροφοριακούς πόρους, πρέπει να τηρούν αρχείο όλων των χρηστών που έχουν πρόσβαση (με απλά ή προνομιακά δικαιώματα). Επίσης, πρέπει να είναι διαθέσιμα όλα τα σχετικά αιτήματα πρόσβασης που έχουν υποβληθεί για τους χρήστες.

2.4 Διαδικασία διαχείρισης προσβάσεων

Προκειμένου να διασφαλιστεί ένα ενιαίο σύστημα πρόσβασης σε όλα τα πληροφοριακά συστήματα της ΕΕΤΤ, εφαρμόζεται μια κατάλληλα τεκμηριωμένη διαδικασία διαχείρισης προσβάσεων, η οποία τηρείται καθ' όλη τη διάρκεια ζωής των πληροφοριακών συστημάτων.

Η διαδικασία αυτή περιλαμβάνει τα ακόλουθα στοιχεία ελέγχου προκειμένου για τη διαχείριση της δημιουργίας, της διαγραφής και της τροποποίησης των λογαριασμών, των κωδικών και των δικαιωμάτων των χρηστών ή και άλλων ενεργειών:

- *Εγγραφή χρήστη. Αποτελεί την τυπική έγκριση και τεκμηρίωση της πρόσβασης των χρηστών στα πληροφοριακά συστήματα.*
- *Αναθεώρηση των δικαιωμάτων πρόσβασης χρήστη. Αποτελεί την τυπική επανεξέταση των εκχωρηθέντων προνομίων που έχουν χορηγηθεί.*

2.5 Εξουσιοδότηση χρήσης

Ο ιδιοκτήτης πληροφοριών (information owner) είναι ο μόνος που μπορεί να εξουσιοδοτήσει με δικαιώματα πρόσβασης τους χρήστες των αντίστοιχων πληροφοριών. Για το σκοπό αυτό, έχει τη δυνατότητα υποβολής ψηφιακού αιτήματος στην εξειδικευμένη εφαρμογή διαχείρισης αιτημάτων υποστήριξης πληροφορικής της ΕΕΤΤ, με το οποίο αιτείται την απόδοση προσβάσεων στους εργαζόμενους. Η υποβολή του αιτήματος αποτελεί το έναυσμα της διαδικασίας. Κατόπιν, το αίτημα, μέσω της εφαρμογής διαχείρισης αιτημάτων, προωθείται κατάλληλα στα αρμόδια στελέχη της Διεύθυνσης Ψηφιακής Διακυβέρνησης για την διεκπεραίωσή του (βλ. το Εγχειρίδιο Διαδικασιών).

2.6 Αρχή "need to know" (ανάγκη γνώσης)

Δικαιώματα πρόσβασης σε ευαίσθητες ή σημαντικές πληροφορίες πρέπει να παρέχονται μόνο στους χρήστες που τις χρειάζονται προκειμένου να εκπληρώσουν τα υπηρεσιακά καθήκοντά τους. Η πρόσβαση τρίτων μερών σε ευαίσθητες ή κρίσιμες πληροφορίες επιτρέπεται μόνο έπειτα από υπογεγραμμένη συμφωνία εμπιστευτικότητας και μη αποκάλυψης πληροφοριών (Non-Disclosure Agreement).

2.7 Αρχή "least privilege" (ελαχίστων προνομίων)

Στους λογαριασμούς χρηστών χορηγείται μόνο το επίπεδο εξουσιοδότησης που είναι απαραίτητο για την εκτέλεση των εργασιών τους (δηλαδή τα ελάχιστα δικαιώματα πρόσβασης). Ο σκοπός είναι περιορίζοντας τις δυνατότητες των λογαριασμών των χρηστών στο ελάχιστο, να ελαχιστοποιηθεί η επιφάνεια μιας ενδεχόμενης επίθεσης και άρα οι πιθανές αρνητικές συνέπειες.

2.8 Αρχή "need to retain" (ανάγκη διατήρησης)

Δικαιώματα πρόσβασης σε ευαίσθητες ή κρίσιμες πληροφορίες πρέπει να παρέχονται μόνο για όσο χρονικό διάστημα είναι απολύτως απαραίτητο. Κατόπιν, τα δικαιώματα αυτά πρέπει να ανακαλούνται. Με κατάλληλες διαδικασίες, η ΕΕΤΤ διασφαλίζει ότι στις περιπτώσεις μεταβολής ή

διακοπής της απασχόλησης του προσωπικού, τα δικαιώματα πρόσβασης τροποποιούνται ανάλογα. Σε κάθε περίπτωση πάντως, εάν το δικαίωμα χρήσης των πληροφοριών ενός χρήστη παρέλθει / ανακληθεί, τότε ο χρήστης πρέπει να αποφύγει τη χρήση των συγκεκριμένων πληροφοριών και να ενημερώσει άμεσα τον προϊστάμενό του.

2.9 Επίπεδο πρόσβασης

Η πρόσβαση ενός χρήστη σε ένα πληροφοριακό σύστημα πρέπει να ελέγχεται σύμφωνα με το επίπεδο εξουσιοδότησης (απλή ή προνομιακή πρόσβαση) που έχει σε αυτό. Το επίπεδο εξουσιοδότησης εξαρτάται από τα δικαιώματα πρόσβασης που του παρέχονται στο σύστημα (βλ. την Πολιτική Διαχείρισης Πληροφοριακών Πόρων).

2.10 Είδος πρόσβασης

Το είδος πρόσβασης εξαρτάται από την κρισιμότητα του πληροφοριακού συστήματος σε συνδυασμό με τη μέθοδο πρόσβασης (βλ. την Πολιτική Διαχείρισης Πληροφοριακών Πόρων):

- *Εσωτερική πρόσβαση: πρόσβαση των χρηστών στα πληροφοριακά συστήματα της ΕΕΤΤ με τη χρήση του δικτύου της.*
- *Απομακρυσμένη πρόσβαση: πρόσβαση των χρηστών στα πληροφοριακά συστήματα της ΕΕΤΤ με τη χρήση εξωτερικού δικτύου της (π.χ. μέσω VPN, δηλαδή Virtual Private Network).*
- *Πρόσβαση σε συστήματα τρίτων μερών: πρόσβαση χρηστών σε πληροφοριακά συστήματα τρίτων μερών με χρήση της υποδομής της ΕΕΤΤ.*

3 Ταυτοποίηση χρήστη

3.1 Μηχανισμοί ελέγχου ταυτότητας χρήστη

Η ταυτοποίηση των χρηστών στα πληροφοριακά συστήματα της ΕΕΤΤ πρέπει να γίνεται με ισχυρές μεθόδους και τεχνολογίες ασφαλούς αυθεντικοποίησης, όπως μέσω:

- *Μηχανισμών που επαληθεύουν τη γνώση ενός ισχυρού μυστικού κωδικού/συνθηματικού*
- *Μηχανισμών που επαληθεύουν την κατοχή ενός ψηφιακού πιστοποιητικού (έξυπνης κάρτας, συσκευής, κτλ.)*

Αυτοί οι μηχανισμοί πρέπει να χρησιμοποιούνται σύμφωνα με το υφιστάμενο ρυθμιστικό/κανονιστικό πλαίσιο και ανάλογα με την ταξινόμηση της κρισιμότητας των πληροφοριακών πόρων.

Ο έλεγχος ταυτότητας χρήστη πριν την πρόσβαση στα πληροφοριακά συστήματα πρέπει να πραγματοποιείται σε ένα ή περισσότερα από τα ακόλουθα επίπεδα, όπου χρειάζεται:

- *Εφαρμογή ή/και βάση δεδομένων*
- *Λειτουργικό σύστημα*
- *Δίκτυο*
- *Domain*

Όλοι οι μηχανισμοί ελέγχου ταυτότητας χρηστών που χρησιμοποιούνται, πρέπει να είναι διεθνώς αναγνωρισμένοι, να ελέγχονται διεξοδικά και να είναι σε γνώση του Υπεύθυνου Ασφάλειας Πληροφοριακών Συστημάτων (ΥΑΠΣ) της ΕΕΤΤ.

3.2 Έλεγχος πρόσβασης βάσει ενός έγκυρου λογαριασμού χρήστη

Ο έλεγχος πρόσβασης στα πληροφοριακά συστήματα της ΕΕΤΤ βασίζεται σε έναν έγκυρο λογαριασμό χρήστη. Η εγκυρότητα του λογαριασμού χρήστη επιτυγχάνεται με την επαλήθευση της ταυτότητάς του.

3.3 Υποδομή διαχείρισης προσβάσεων χρηστών

Εφόσον είναι δυνατό, οι μηχανισμοί ασφάλειας λογικής πρόσβασης χρησιμοποιούν μια κεντρική υποδομή διαχείρισης πρόσβασης. Η υποδομή αυτή αρνείται κάθε πρόσβαση ως προεπιλογή, ώστε να διασφαλίζει ότι κανένας δεν έχει πρόσβαση έως ότου εφαρμοστεί η κατάλληλη πολιτική που το επιτρέπει.

3.4 Έλεγχος ταυτότητας χρήστη για πρόσβαση σε εξωτερικά δίκτυα

Ο εσωτερικός έλεγχος ταυτότητας χρήστη επιβάλλεται τουλάχιστον για το λειτουργικό σύστημα (π.χ. επιτυχής έλεγχος ταυτότητας στον υπολογιστή του χρήστη), προτού παραχωρηθεί πρόσβαση σε εξωτερικά δίκτυα (π.χ. στο Διαδίκτυο).

4 Διαχείριση λογαριασμού/ονόματος χρήστη

4.1 Διαδικασία Διαχείρισης Χρηστών

Οι λογαριασμοί χρηστών εκχωρούνται σε συγκεκριμένους χρήστες μόνο κατόπιν έγκρισης. Έχει τεθεί σε εφαρμογή ένας κεντρικός τρόπος διαχείρισης των αιτημάτων πρόσβασης και είναι δυνατή η δημιουργία προκαθορισμένων προφίλ χρήστη. Τα δικαιώματα πρόσβασης σε επίπεδο συστήματος και εφαρμογών, καθώς και όλα τα δικαιώματα απομακρυσμένης πρόσβασης που αφορούν απλή ή προνομιακή πρόσβαση χρηστών εγκρίνονται και ελέγχονται.

Το Τμήμα Ανθρώπινου Δυναμικού πρέπει, με υποβολή ψηφιακού αιτήματος στην εξειδικευμένη εφαρμογή διαχείρισης αιτημάτων υποστήριξης πληροφορικής, να ενημερώνει τη Διεύθυνση Ψηφιακής Διακυβέρνησης για τα νέα στελέχη (μέλη της Διοίκησης, προϊσταμένους, εργαζόμενους, ασκούμενους δικηγόρους κ.λπ.), όπως και αυτά που επέστρεψαν από μακροχρόνια απουσία, προκειμένου να εκτελούνται όλες οι απαραίτητες ενέργειες δημιουργίας λογαριασμών ή ενεργοποίησης χρηστών, καθώς και απόδοσης προσβάσεων στα πληροφοριακά συστήματα της ΕΕΤΤ. (Βλ. στο Εγχειρίδιο Διαδικασιών της ΕΕΤΤ, τις διαδικασίες εκτέλεσης εργασιών κατά την πρόσληψη προσωπικού, απόδοσης προσβάσεων σε νέο υπάλληλο, καθώς και απόδοσης προσβάσεων σε υπάλληλο που επιστρέφει από μακροχρόνια απουσία.)

4.2 Απενεργοποίηση λογαριασμών/ονομάτων χρηστών

Οι λογαριασμοί των χρηστών απενεργοποιούνται / κλειδώνονται / καταργούνται κατάλληλα σε περιπτώσεις τερματισμού της απασχόλησης ή της σύμβασης βάσει της οποίας αποκτήθηκε ο λογαριασμός / δικαίωμα πρόσβασης.

Κατά τη διάρκεια έρευνας σχετικά με κάποιο περιστατικό ασφάλειας, ορισμένοι λογαριασμοί χρηστών ενδέχεται να απενεργοποιηθούν. Σε αυτές τις περιπτώσεις, ένα αίτημα χρήστη ή διαχειριστή για επανενεργοποίηση του λογαριασμού είναι επαρκές. Θα πρέπει ωστόσο να δοθούν περαιτέρω εξηγήσεις για τους λόγους που οδήγησαν στην απενεργοποίηση και εφόσον κριθούν ικανοποιητικές, ο λογαριασμός μπορεί να επανενεργοποιηθεί.

Σε περιπτώσεις λήξης της εργασιακής σχέσης, η πρόσβαση ανακαλείται οριστικά.

4.3 Μοναδικότητα λογαριασμού/ονόματος χρήστη

Η ΕΕΤΤ χορηγεί μοναδική ταυτότητα (identity) σε κάθε χρήστη για κάθε σύστημα που αποκτά πρόσβαση. Έτσι όλοι οι χρήστες (διαχειριστές, προγραμματιστές, απλοί χρήστες κτλ.) που έχουν πρόσβαση στα πληροφοριακά συστήματα της ΕΕΤΤ έχουν ένα μοναδικό λογαριασμό χρήστη, ο οποίος χρησιμοποιείται μόνο από αυτούς. Με τον τρόπο αυτό, είναι δυνατός ο εντοπισμός του χρήστη που είναι υπεύθυνος για τις ενέργειες που εκτελούνται σε κάθε πληροφοριακό σύστημα, με σκοπό τη διασφάλιση της λογοδοσίας.

Κοινόχρηστοι λογαριασμοί χρηστών δεν χρησιμοποιούνται. Μόνο υπό ειδικές περιστάσεις και εφόσον κριθεί απολύτως απαραίτητο από την ΕΕΤΤ, μία ομάδα χρηστών μπορεί να μοιράζεται τον ίδιο λογαριασμό για να εκτελεί συγκεκριμένες εργασίες σε κάποιο πληροφοριακό σύστημα. Πρέπει, ωστόσο, να υπάρχει ένας υπεύθυνος για αυτούς τους κοινόχρηστους λογαριασμούς (π.χ. ο προϊστάμενος της οργανικής μονάδας).

4.4 Χρήση ειδικών λογαριασμών

Πριν τη μεταφορά ενός συστήματος στο περιβάλλον παραγωγής, όλοι οι μη χρησιμοποιούμενοι ή οι προεπιλεγμένοι λογαριασμοί χρηστών (π.χ. λογαριασμοί επισκεπτών κτλ.) πρέπει να διαγράφονται ή να απενεργοποιούνται στην περίπτωση που η διαγραφή τους δεν είναι εφικτή. Σε περίπτωση που δεν είναι εφικτή ούτε η απενεργοποίηση ούτε η διαγραφή, ο προεπιλεγμένος κωδικός πρόσβασης πρέπει να αλλάξει.

Οι λογαριασμοί διαχειριστών πρέπει να μετονομάζονται, έτσι ώστε να μπορούν δύσκολα να προβλεφθούν. Σε περίπτωση που ο προμηθευτής του συστήματος πρέπει να έχει τακτική πρόσβαση στο πληροφοριακό σύστημα, πρέπει να του ανατεθεί ένας μοναδικός λογαριασμός με τα κατάλληλα δικαιώματα, από τον αρμόδιο διαχειριστή, σύμφωνα με τη σχετική πολιτική (βλ. την Πολιτική Διαχείρισης Τρίτων Μερών).

4.5 Απαιτήσεις ασφάλειας λογαριασμού/ονόματος χρήστη

Πρέπει να αποφεύγονται ονόματα λογαριασμών που υπονοούν / αποκαλύπτουν τη θέση που κατέχει ο χρήστης στην ΕΕΤΤ.

5 Διαχείριση κωδικών πρόσβασης

5.1 Απόκρυψη κωδικού πρόσβασης

Κατά τη διάρκεια της διαδικασίας σύνδεσης στα πληροφοριακά συστήματα της ΕΕΤΤ, ο κωδικός πρόσβασης πρέπει να αποκρύπτεται από το χρήστη, προκειμένου να μην υποκλαπεί μέσω της μεθόδου του κρυφού κοιτάγματος (shoulder surfing), κατά την οποία κάποιος τρίτος αποσπά ευαίσθητες πληροφορίες παρατηρώντας την οθόνη ή το πληκτρολόγιο του χρήστη.

5.2 Δημιουργία και αλλαγή των κωδικών πρόσβασης

Οι κωδικοί πρόσβασης που χρησιμοποιούνται για τα πληροφοριακά συστήματα της ΕΕΤΤ πρέπει να επιλέγονται από τους χρήστες. Η ισχύς του κωδικού πρόσβασης πρέπει να επιβάλλεται από το εκάστοτε πληροφοριακό σύστημα.

Ο αρχικός κωδικός πρόσβασης πρέπει να είναι έγκυρος μόνο για την αρχική σύνδεση στο σύστημα. Κατά την αρχική σύνδεση, ο χρήστης υποχρεούται να αλλάξει τον αρχικό κωδικό πρόσβασης.

5.3 Όριο των διαδοχικών αποτυχημένων προσπαθειών σύνδεσης

Για να περιοριστεί η πιθανότητα κάποιος τρίτος να μαντέψει τον κωδικό πρόσβασης έγκυρου χρήστη ενός συστήματος, ο αριθμός των διαδοχικών προσπαθειών σύνδεσης πρέπει να είναι αυστηρά περιορισμένος. Ο λογαριασμός πρέπει να κλειδώνει μετά από το πολύ πέντε (5) συνεχείς αποτυχημένες προσπάθειες πρόσβασης για τα κρίσιμα συστήματα, εφόσον αυτό είναι εφικτό. Όταν ο λογαριασμός ενός χρήστη κλειδώσει, παραμένει κλειδωμένος για μία προκαθορισμένη χρονική περίοδο (π.χ. 30 λεπτά) ή έως ότου ο διαχειριστής του συστήματος ξεκλειδώσει το λογαριασμό.

Σε περιπτώσεις που το παραπάνω δεν είναι εφικτό για κάποιο πληροφοριακό σύστημα ή εφαρμογή, γιατί δεν μπορεί να το υποστηρίξει, πρέπει να εφαρμοστούν άλλες πρακτικές ασφαλείας, όπως το Web Application Firewall (WAF), το οποίο είναι μια μορφή αναχώματος ασφαλείας (firewall) που ελέγχει την είσοδο / έξοδο ή τις κλήσεις συστήματος μιας διαδικτυακής εφαρμογής ή υπηρεσίας, ή εναλλακτικά να εφαρμόζονται άλλοι μηχανισμοί ασφάλειας.

5.4 Κρυπτογράφηση κωδικού πρόσβασης

Οι κωδικοί πρόσβασης πρέπει πάντα να κρυπτογραφούνται ή να έχουν κατακερματιστεί κατά την αποθήκευση ή τη μεταβίβασή τους μέσω δικτύων, ώστε να μην αποκαλύπτονται σε μη εξουσιοδοτημένους χρήστες. Για την κρυπτογράφηση, πρέπει να χρησιμοποιούνται διεθνώς αναγνωρισμένοι αλγόριθμοι. Επιπλέον, τα πληροφοριακά συστήματα πρέπει να σχεδιάζονται και να ελέγχονται έτσι ώστε να διασφαλίζεται ότι η ανάκτηση κρυπτογραφημένων ή μη κωδικών πρόσβασης δεν είναι δυνατή.

5.5 Αποθήκευση κωδικού πρόσβασης

Οι κωδικοί πρόσβασης δεν πρέπει να αποθηκεύονται σε οποιαδήποτε μορφή σε συστήματα στα οποία δεν υπάρχει έλεγχος πρόσβασης, συμπεριλαμβανομένων των εγγράφων, των μακροεντολών λογισμικού, των φυλλομετρητών ιστού (web browsers) κτλ. Ενδεικτικά, μπορούν να υποκλαπούν με άμεσο τρόπο οι αποθηκευμένοι κωδικοί από τη μνήμη του web browser χωρίς ο χρήστης να το αντιληφθεί και μάλιστα με τη χρήση των δικαιωμάτων απλού χρήστη (δεν απαιτούνται προνόμια διαχειριστή). Για λόγους ασφαλείας, η ΕΕΤΤ διατηρεί το δικαίωμα να διαγράφει αποθηκευμένους κωδικούς.

5.6 Αποκάλυψη κωδικών πρόσβασης

Όλοι οι κωδικοί πρόσβασης ενός συστήματος πρέπει να αλλάζουν άμεσα εάν υπάρχει υποψία ή απόδειξη ότι αποκαλύφθηκαν σε μη εξουσιοδοτημένους χρήστες.

5.7 Απαιτήσεις ασφάλειας κωδικού πρόσβασης

Οι κωδικοί πρόσβασης χρηστών και διαχειριστών πρέπει να τηρούν τα πρότυπα και τις καλές πρακτικές ασφάλειας όσον αφορά στο μήκος, την πολυπλοκότητα, το ιστορικό και την περίοδο ισχύος. Όλοι οι κωδικοί πρόσβασης πρέπει να ικανοποιούν τις συγκεκριμένες απαιτήσεις που καθορίζονται στην Πολιτική Ασφάλειας της ΕΕΤΤ. Εάν είναι δυνατό, τα πληροφοριακά συστήματα της ΕΕΤΤ πρέπει να εφαρμόζουν αυτόματα αυτό το πρότυπο, διαφορετικά οι χρήστες πρέπει από μόνοι τους να ακολουθούν τους παραπάνω περιορισμούς ως προς το μήκος, την πολυπλοκότητα κτλ. Οποιαδήποτε απόκλιση από τους ανωτέρω κανόνες πρέπει να τεκμηριώνεται και να εγκρίνεται.

Για την αποτελεσματικότερη διαχείριση των κωδικών, συνιστάται η χρήση του εξειδικευμένου συστήματος διαχείρισης κωδικών πρόσβασης που προτείνει η Διεύθυνση Ψηφιακής Διακυβέρνησης.

6 Έλεγχοι ασφάλειας για προνομιακούς χρήστες

6.1 Προνομιακή πρόσβαση στα συστήματα

Τα δικαιώματα πρόσβασης για την τροποποίηση των ρυθμίσεων διαχείρισης, συντήρησης και διαμόρφωσης στα πληροφοριακά συστήματα της ΕΕΤΤ πρέπει:

- *Να χορηγούνται μόνο σε εξουσιοδοτημένους υπαλλήλους μετά από κατάλληλες εγκρίσεις.*
- *Να περιορίζονται μόνο στα λιγότερα δυνατά προνόμια και στον απόλυτα απαραίτητο βαθμό, με βάση την κρισιμότητα των υπηρεσιακών λειτουργιών ή αρμοδιοτήτων της ΕΕΤΤ, κατά περίπτωση, καθώς και το σχήμα ταξινόμησης των πληροφοριακών πόρων της.*
- *Να ανατίθενται σε διαχειριστές με βάση την ταξινόμηση της εκάστοτε εργασίας.*

6.2 Περιορισμός προνομιακών λογαριασμών

Οι προνομιακοί λογαριασμοί χρηστών πρέπει να παρέχονται μόνο στους υπεύθυνους για τη διαχείριση και την ασφάλεια του εκάστοτε συστήματος.

Οι λογαριασμοί με διαχειριστικά προνόμια πρέπει να αντιστοιχούν σε τουλάχιστον δύο άτομα ανά σύστημα και ο διαχωρισμός των καθηκόντων πρέπει να επιβάλλεται για τους διαχειριστές. Η ύπαρξη ενός δεύτερου εργαζομένου ως διαχειριστή εμποδίζει αδικαιολόγητες διακοπές της υπηρεσίας και περιορίζει την πιθανότητα εμφάνισης ανάρμοστων ενεργειών του άλλου υπαλλήλου.

6.3 Χορήγηση διαχειριστικών προνομίων σε λογαριασμούς απλών χρηστών

Δεν πρέπει να χορηγούνται διαχειριστικά προνόμια σε λογαριασμούς απλών χρηστών εκτός εάν υπάρχει σχετική εξουσιοδότηση.

6.4 Από κοινού πρόσβαση σε προνομιακούς λογαριασμούς

Η από κοινού πρόσβαση σε προνομιακούς λογαριασμούς απαγορεύεται. Μπορεί να επιτραπεί μόνο υπό την προϋπόθεση διεξαγωγής κατάλληλων ελέγχων και έπειτα από ρητή έγκριση.

6.5 Πρόσβαση σε προνομιακούς λογαριασμούς μέσω ασφαλών πρωτοκόλλων

Η πρόσβαση σε κρίσιμα συστήματα μέσω προνομιακών λογαριασμών πρέπει να πραγματοποιείται μέσω ασφαλών πρωτοκόλλων.

6.6 Ελεγχόμενη πρόσβαση στον πηγαίο κώδικα

Η πρόσβαση στον πηγαίο κώδικα πρέπει να ελέγχεται αυστηρά και να χορηγείται μόνο εάν προηγουμένως έχει εγκριθεί από τους αντίστοιχους ιδιοκτήτες πληροφοριών ή εάν υπάρχει νόμιμη ανάγκη.

6.7 Ανάπτυξη λογισμικού και διαχωρισμός πρόσβασης

Συνιστάται οι χρήστες που συμμετέχουν στην ανάπτυξη και συντήρηση εφαρμογών να μην έχουν πλήρη πρόσβαση στο περιβάλλον παραγωγής των συστημάτων, εφόσον είναι εφικτό. Η πρόσβαση με δικαιώματα ανάγνωσης θα πρέπει να επιτρέπεται έτσι ώστε να διασφαλίζεται ότι τα περιστατικά ή/και τα προβλήματα των χρηστών αντιμετωπίζονται άμεσα.

Συνιστάται, εφόσον είναι εφικτό, ο ρόλος του διαχειριστή και ο ρόλος του προγραμματιστή να μην συγκεντρώνονται στο ίδιο άτομο.

6.8 Πρόσβαση στους ηλεκτρονικούς υπολογιστές των εργαζομένων

Η πρόσβαση των αρμόδιων στελεχών της Διεύθυνσης Ψηφιακής Διακυβέρνησης στον ηλεκτρονικό υπολογιστή (remote desktop) ενός εργαζόμενου για λόγους τεχνικής υποστήριξης, διενεργείται μόνο μετά από σχετικό αίτημα υποστήριξης του ίδιου του εργαζόμενου.

7 Διαχείριση κωδικών προνομιακών λογαριασμών

7.1 Πρόσβαση σε κωδικούς προνομιακών λογαριασμών

Η πρόσβαση σε ευαίσθητα συστήματα πρέπει να παρέχεται μέσω της χρήσης ενός συστήματος διαχείρισης κωδικών πρόσβασης, όπου είναι εφικτό. Ένα τέτοιο σύστημα επιβάλλει τον έλεγχο ταυτότητας χρήστη χρησιμοποιώντας τα μοναδικά διαπιστευτήριά του.

Το σύστημα πρέπει να καταγράφει την εγγραφή πρόσβασης του χρήστη για σκοπούς ελέγχου.

7.2 Δημιουργία έκτακτου διαχειριστικού λογαριασμού πρόσβασης σε κρίσιμα πληροφοριακά συστήματα για χρήση σε κατάσταση έκτακτης ανάγκης

Για τα κρίσιμα πληροφοριακά συστήματα της ΕΕΤΤ, η απομακρυσμένη πρόσβαση θα πρέπει να γίνεται με χρήση μεθόδων αυξημένης ασφάλειας (ssh κλειδιών με passphrases για τα linux μηχανήματα και μηχανισμών πρόσβασης πολλαπλών παραγόντων (Multi-Factor Authentication ή MFA) για τα Windows συστήματα). Θα πρέπει, ωστόσο, να υπάρχει σε κάθε σύστημα ένας διαχειριστικός λογαριασμός έκτακτης ανάγκης (last resort) ο οποίος θα χρησιμοποιείται μόνο στην περίπτωση που η πρόσβαση με τα αυξημένα μέτρα δεν είναι εφικτή για κάποιο τεχνικό λόγο. Το συνθηματικό (password) του λογαριασμού αυτού θα αλλάζει μετά τη χρήση του και θα φυλάσσεται σε κρυπτογραφημένο αρχείο κωδικών.

8 Άλλα μέτρα ελέγχου πρόσβασης

8.1 Παρακολούθηση ασφάλειας συστημάτων

Σύμφωνα με την ισχύουσα νομοθεσία, η ΕΕΤΤ διατηρεί το δικαίωμα, για λόγους ασφαλείας, να καταγράφει και να παρακολουθεί τις ενέργειες των χρηστών που χρησιμοποιούν τα πληροφοριακά συστήματά της. Λεπτομέρειες για τις σχετικές πολιτικές που εφαρμόζει και τις τεχνολογίες που χρησιμοποιεί για την παρακολούθηση της ασφάλειας, αναφέρονται στην Πολιτική Παρακολούθησης Ασφάλειας Συστημάτων.

8.2 Μη επιτηρούμενοι υπολογιστές και τερματικά

Οι υπολογιστές και οι τερματικοί σταθμοί πρέπει να παραμένουν αποσυνδεδεμένοι ή να προστατεύονται με μηχανισμό κλειδώματος οθόνης και πληκτρολογίου που ελέγχεται από έναν κωδικό πρόσβασης, ένα διακριτικό ή παρόμοιο μηχανισμό ελέγχου ταυτότητας χρήστη, όταν δεν επιτηρούνται.

8.3 Αυτόματη αποσύνδεση από τα συστήματα

Οι συνδέσεις (συμπεριλαμβανομένων των απομακρυσμένων συνδέσεων) σε συστήματα που έχουν παραμείνει ανενεργά για προκαθορισμένο χρονικό διάστημα πρέπει να τερματίζονται.

Ο χρήστης/διαχειριστής πρέπει να είναι σε θέση να αποκαταστήσει τη σύνδεση μόνο μετά την πληκτρολόγηση ενός ονόματος χρήστη και ενός κωδικού πρόσβασης.

Εξαιρούνται των ανωτέρω κανόνων τα συστήματα που βρίσκονται σε λειτουργία παρακολούθησης για λόγους ασφαλείας.

8.4 Σφάλματα ειδοποίησης στον έλεγχο ταυτότητας χρήστη

Οι χρήστες/διαχειριστές πρέπει να ενημερώνονται μόνο για την αποτυχία της προσπάθειας σύνδεσης. Τα πληροφοριακά συστήματα δεν πρέπει να παρέχουν άλλες πληροφορίες (π.χ. τύπος συστήματος, έκδοση λειτουργικού, κλπ.).

8.5 Απαγόρευση εμφάνισης της τελευταίας σύνδεσης

Κατά τη διάρκεια ελέγχου ταυτότητας, το σύστημα δεν πρέπει να εμφανίζει τον προηγούμενο λογαριασμό/όνομα χρήστη που χρησιμοποιήθηκε για την επιτυχή σύνδεση στο σύστημα.

9 Αναθεώρηση των δικαιωμάτων πρόσβασης

9.1 Αναθεώρηση των δικαιωμάτων πρόσβασης

Οι λογαριασμοί χρηστών και τα δικαιώματα πρόσβασης σε κρίσιμα ή ευαίσθητα πληροφοριακά συστήματα πρέπει να επανεξετάζονται σε τακτική βάση (π.χ. εξαμηνιαίως) (Βλ. τη διαδικασία περιοδικής επισκόπησης προσβάσεων στο Εγχειρίδιο Διαδικασιών της ΕΕΤΤ). Στο πλαίσιο αυτό, η μη έγκαιρη απόκριση προϊσταμένου σε αίτημα του αρμόδιου στελέχους της Διεύθυνσης Ψηφιακής Διακυβέρνησης να ελεγχθούν οι προσβάσεις του προσωπικού της οργανικής μονάδας και να υποβληθούν ψηφιακά αιτήματα για τις απαιτούμενες αλλαγές εντός

συγκεκριμένης προθεσμίας, θα εκλαμβάνεται, με ευθύνη του προϊσταμένου, ως μη ύπαρξη τέτοιων αλλαγών πρόσβασης.

Τα προνόμια πρέπει να αναθεωρούνται εάν οι απαιτήσεις ή υπηρεσιακές ευθύνες / αρμοδιότητες αλλάζουν, έτσι ώστε να συνάδουν με τις πραγματικές υπηρεσιακές λειτουργίες. Οι εργαζόμενοι οφείλουν να ενημερώνουν του προϊσταμένους τους εφόσον διατηρούν επιπλέον δικαιώματα πρόσβασης από αυτά που απαιτούνται σύμφωνα με τις αρμοδιότητές τους. Οι προϊστάμενοι πρέπει να υποβάλλουν αμελλητί τα ψηφιακά αιτήματά τους για την αλλαγή προσβάσεων μέσω της εξειδικευμένης εφαρμογής διαχείρισης αιτημάτων υποστήριξης πληροφορικής, προκειμένου η Διεύθυνση Ψηφιακής Διακυβέρνησης να δρομολογεί τις απαραίτητες ενέργειες διεκπεραίωσης των αλλαγών.

Επισημαίνεται ότι ο περιοδικός έλεγχος των δικαιωμάτων πρόσβασης είναι ένα από τα κρίσιμα πεδία κατά τους ελέγχους ασφάλειας πληροφοριών που πρέπει να διενεργείται σύμφωνα με την Πολιτική Διενέργειας Ελέγχων Ασφάλειας Πληροφοριών.

9.2 Μετακινήσεις ή αποχωρήσεις εργαζομένων

Το Τμήμα Ανθρώπινου Δυναμικού πρέπει, με υποβολή ψηφιακού αιτήματος στην εξειδικευμένη εφαρμογή διαχείρισης αιτημάτων υποστήριξης πληροφορικής, να ενημερώνει τη Διεύθυνση Ψηφιακής Διακυβέρνησης για τις μακροχρόνιες ή οριστικές αποχωρήσεις ή τις μετακινήσεις εργαζομένων σε νέα θέση ή θέση προϊσταμένου, προκειμένου να γίνονται όλες οι απαραίτητες ενέργειες σχετικά με την αναθεώρηση των προνομίων λογικής πρόσβασης στα πληροφοριακά συστήματα της ΕΕΤΤ. (Βλ. στο Εγχειρίδιο Διαδικασιών της ΕΕΤΤ, τη διαδικασία εκτέλεσης εργασιών κατά την αποχώρηση, αλλαγή προσωπικού, καθώς και τη διαδικασία απόδοσης προσβάσεων κατά τη μετακίνηση υπαλλήλου σε νέα θέση ή θέση προϊσταμένου.)

9.3 Απενεργοποίηση και κατάργηση δικαιωμάτων πρόσβασης

Στις περιπτώσεις που η υπηρεσιακή σχέση μεταξύ της ΕΕΤΤ και ενός υπαλλήλου ή ενός εξωτερικού συνεργάτη (π.χ. ασκούμενου δικηγόρου) διακόπτεται προσωρινά, λόγω μακροχρόνιας αποχώρησης, τότε πρέπει να απενεργοποιούνται τα δικαιώματα λογικής πρόσβασης σε εφαρμογές, κοινόχρηστους φακέλους, ομαδικά email και επίσης να απενεργοποιείται ο χρήστης από το VPN. Κατά τη μακροχρόνια αποχώρηση, το email του εργαζόμενου παραμένει ενεργό ενώ ρυθμίζεται η αυτόματη απόκριση που ειδοποιεί για την απουσία του (out-of-office auto-reply) και μειώνεται το όριο της χωρητικότητας του mailbox του. Εάν η αποχώρηση είναι οριστική, τότε οι λογαριασμοί χρήστη και τα δικαιώματα πρόσβασης πρέπει να απενεργοποιούνται ή καταργούνται κατάλληλα και να διαγράφεται το email του. (Βλ. στο Εγχειρίδιο Διαδικασιών της ΕΕΤΤ, τις διαδικασίες απενεργοποίησης προσβάσεων σε μακροχρόνια και σε οριστική αποχώρηση.)

9.4 Λήξη συνεργασίας με τρίτα μέρη

Σε περίπτωση που σε κάποιο τρίτο μέρος ανατεθεί η εκτέλεση ενός έργου της ΕΕΤΤ, μετά την περάτωση αυτού, ο Ιδιοκτήτης Πληροφοριών πρέπει να ενημερώνει τη Διεύθυνση Ψηφιακής Διακυβέρνησης και τα λοιπά εμπλεκόμενα μέρη για τη λήξη της συνεργασίας, προκειμένου να ανακληθούν οι προσβάσεις στα πληροφοριακά συστήματα της ΕΕΤΤ.

10 Απομακρυσμένη πρόσβαση

10.1 Αρχές απομακρυσμένης πρόσβασης

Η απομακρυσμένη πρόσβαση στο δίκτυο της ΕΕΤΤ πρέπει να υλοποιείται με τέτοιο τρόπο, ώστε:

- *Να παρέχεται μόνο όταν έχουν ληφθεί τα απαιτούμενα μέτρα ασφαλείας.*
- *Να περιορίζεται στις ελάχιστες υπηρεσίες, συστήματα, λειτουργίες και πληροφορίες που απαιτούνται για την εκτέλεση της εκάστοτε υπηρεσιακής διαδικασίας.*
- *Να χρησιμοποιείται μόνο από συγκεκριμένους εξουσιοδοτημένους χρήστες.*
- *Να χρησιμοποιούνται μόνο εγκεκριμένα προϊόντα και υπηρεσίες.*
- *Η πρόσβαση στο δίκτυο να περιορίζεται μόνο στα απαιτούμενα εσωτερικά πληροφοριακά συστήματα.*
- *Οι απομακρυσμένες επικοινωνίες να είναι κρυπτογραφημένες.*

10.2 Στόχοι Μηχανισμών Απομακρυσμένης Πρόσβασης

Όλοι οι μηχανισμοί ελέγχου απομακρυσμένης πρόσβασης της ΕΕΤΤ έχουν τουλάχιστον τους ακόλουθους στόχους:

- *Υποστήριξη μόνο έμμεσης πρόσβασης σε εσωτερικά συστήματα πληροφοριών ή / και συσκευές δικτύου της ΕΕΤΤ (π.χ. μέσω μηχανισμών ασφαλείας, όπως αναχωμάτων ασφαλείας, μηχανισμών VPN κ.λπ.)*
- *Έλεγχος ταυτότητας χρηστών μόνο βάσει ενός σχήματος ελέγχου ταυτότητας δύο παραγόντων (two factor authentication), το οποίο απαιτεί δύο διαφορετικές μορφές ταυτοποίησης για την πρόσβαση. Προσθέτει, δηλαδή, ένα επιπλέον επίπεδο επαλήθευσης πέρα από τον απλό κωδικό πρόσβασης, όπως την επαλήθευση μέσω ειδικής εφαρμογής στο κινητό τηλέφωνο.*

10.3 Εμπιστευτικότητα των πληροφοριών πρόσβασης

Οι πληροφορίες σχετικά με την πρόσβαση των χρηστών σε πληροφοριακά συστήματα, όπως οι διευθύνσεις IP (Internet Protocol Address), οι διευθύνσεις URL (Uniform Resource Locator), θεωρούνται πληροφορίες μόνο για εσωτερική χρήση. Αυτού του είδους οι πληροφορίες δεν αποκαλύπτονται σε τρίτα μέρη για κανένα λόγο, εκτός εάν απαιτείται από τη νομοθεσία.

10.4 Επιλογή και χρήση μηχανισμών ελέγχου ασφάλειας απομακρυσμένης πρόσβασης

Σε περιπτώσεις που παρέχεται απομακρυσμένη πρόσβαση στους χρήστες, χρησιμοποιούνται τουλάχιστον οι ίδιοι μηχανισμοί ασφαλείας, με αυτούς που χρησιμοποιούνται για την πρόσβαση στο εσωτερικό δίκτυο της ΕΕΤΤ.

Η επιλογή των κατάλληλων μηχανισμών ασφαλείας γίνεται μόνο μετά από ανάλυση των σχετικών κινδύνων. Η ισχύς των μηχανισμών αυτών είναι ανάλογη με το επίπεδο κρισιμότητας των δεδομένων και κατ' επέκταση του συστήματος που αυτά τα δεδομένα περιέχονται και στο οποίο παρέχεται η απομακρυσμένη πρόσβαση.

10.5 Περιορισμοί απομακρυσμένης πρόσβασης

Η απομακρυσμένη πρόσβαση στα πληροφοριακά συστήματα της ΕΕΤΤ γίνεται σύμφωνα με τις σχετικές διαδικασίες και τα πρότυπα πρόσβασης της ΕΕΤΤ. Ειδικότερα, προκειμένου για την τηλεργασία του προσωπικού της ΕΕΤΤ, ισχύει η Πολιτική Τηλεργασίας και Φορητών Συσκευών.

10.6 Υποδομή περιβάλλοντος χρήστη

Η απομακρυσμένη πρόσβαση υλοποιείται αποκλειστικά μέσω των ελεγχόμενων υποδομών περιβάλλοντος χρήστη (π.χ. terminal services, κτλ.), οι οποίες έχουν διαμορφωθεί έτσι ώστε να παρέχουν πρόσβαση μόνο στις απαιτούμενες υπηρεσίες και πληροφοριακά συστήματα.

10.7 Έλεγχοι ασφάλειας

Υπάρχει κατάλληλη υποδομή ασφαλείας που διασφαλίζει ότι οι "hosts" (π.χ. φορητοί υπολογιστές κτλ.) που συνδέονται απομακρυσμένα στο δίκτυο της ΕΕΤΤ ελέγχονται πριν αποκτήσουν πρόσβαση στα στοιχεία του δικτύου (π.χ. μέσω χρήσης ενημερωμένου antivirus, εγκατάστασης ενημερώσεων ασφαλείας κτλ.).

10.8 Εποπτεία και λογοδοσία

Οι δραστηριότητες των χρηστών κατά την απομακρυσμένη πρόσβασή τους πρέπει να καταγράφονται στο μέγιστο βαθμό. Πιο συγκεκριμένα, καταγράφονται τα ακόλουθα, όπου αυτό είναι εφικτό:

- *Οι επιτυχείς και ανεπιτυχείς προσπάθειες πρόσβασης στα συστήματα.*
- *Οι δραστηριότητες των χρηστών στο περιβάλλον «ελεγχόμενου χρήστη», εάν χρησιμοποιείται.*
- *Οι δραστηριότητες των χρηστών στα προσβάσιμα συστήματα.*

10.9 Ευθύνες χρήστη

Όλοι οι χρήστες που συνδέονται σε εσωτερικά δίκτυα της ΕΕΤΤ μέσω μηχανισμών απομακρυσμένης πρόσβασης χρησιμοποιούν ενημερωμένο λογισμικό antivirus και antispyware, καθώς και firewall. Οι χρήστες, επίσης, υποχρεούνται να συμμορφώνονται με την Πολιτική Ασφαλείας της ΕΕΤΤ.

11 Λογαριασμοί βάσης δεδομένων και απαιτήσεις κωδικών πρόσβασης

11.1 Κωδικοί hard-coded

Οι κωδικοί που έχουν κωδικοποιηθεί "hard coded", δηλαδή είναι ενσωματωμένοι απευθείας στον πηγαίο κώδικα μιας εφαρμογής, πρέπει να αποφεύγονται, προκειμένου να μην υπάρχει ο κίνδυνος αποκάλυψής τους και μη εξουσιοδοτημένης τροποποίησής τους.

11.2 Προκαθορισμένοι λογαριασμοί

Οι προκαθορισμένοι λογαριασμοί διαχείρισης και οι κωδικοί πρόσβασης σε εφαρμογές/βάσεις δεδομένων πρέπει να μετονομάζονται και να τροποποιούνται αντίστοιχα, πριν από την εγκατάσταση της εφαρμογής στο περιβάλλον παραγωγής.

11.3 Δικαιώματα αρχείων και καταλόγου

Οι διαχειριστές της ΕΕΤΤ πρέπει να διασφαλίζουν ότι τα κρίσιμα αρχεία των βάσεων δεδομένων και οι κατάλογοι δεν είναι προσβάσιμα από απλούς χρήστες και τα σχετικά δικαιώματα ελέγχονται τακτικά.

11.4 Αποθήκευση κωδικών πρόσβασης

Οι βάσεις δεδομένων δεν πρέπει να περιέχουν διαπιστευτήρια χρήστη (π.χ. κωδικούς πρόσβασης). Εάν όμως κωδικοί πρόσβασης αποθηκεύονται σε μία βάση δεδομένων (λόγω του ότι επιχειρησιακά δεν μπορεί να υποστηριχθεί άλλη μέθοδος), τότε θα πρέπει να ισχύουν τα εξής:

- *Κάθε κωδικός πρόσβασης θα πρέπει να έχει κατακερματιστεί (με βάση έναν ασφαλή αλγόριθμο κατακερματισμού).*
- *Μόνο τα αποτελέσματα της διαδικασίας κατακερματισμού θα πρέπει να αποθηκευτούν στη βάση δεδομένων.*
- *Μόνο οι εξαιρετικά προνομιακοί χρήστες θα πρέπει να έχουν πρόσβαση στους κωδικούς πρόσβασης.*

11.5 Απομακρυσμένη πρόσβαση στη βάση δεδομένων

Οι απομακρυσμένες συνδέσεις σε διακομιστές βάσης δεδομένων (database servers) από διαχειριστές με τη χρήση λογισμικού ή μηχανισμών που υποστηρίζονται από ασθενή πρωτόκολλα ελέγχου ταυτότητας και κρυπτογράφησης απαγορεύονται, δεδομένου ότι τα διαπιστευτήρια διαχείρισης μπορεί να διαβιβαστούν από ένα μη ασφαλές κανάλι επικοινωνίας και να χρησιμοποιηθούν από κάποιον κακόβουλο χρήστη που θα θέσει σε κίνδυνο τον διακομιστή της βάσης δεδομένων.

Για να διασφαλιστούν οι υποστηριζόμενοι σύνοδοι (sessions) διαχείρισης, η απομακρυσμένη πρόσβαση σε διακομιστές των βάσεων δεδομένων πρέπει να εφαρμόζεται μόνο όταν:

- *Έχει εφαρμοστεί ισχυροποίηση του επιπέδου ασφάλειας του διακομιστή σύμφωνα με τα τεχνικά πρότυπα και τις οδηγίες της ΕΕΤΤ.*
- *Το λειτουργικό σύστημα του διακομιστή της βάσης δεδομένων έχει υποστεί ισχυροποίηση του επιπέδου ασφάλειας μέσω των τελευταίων ενημερώσεων κώδικα που παρέχονται από τον προμηθευτή.*
- *Γίνεται χρήση μηχανισμών/πρωτοκόλλων κρυπτογράφησης (π.χ. SSH, SSL, RD μέσω SSH κτλ.).*

11.6 Απαιτήσεις πολιτικής κωδικού πρόσβασης βάσης δεδομένων

Οι κωδικοί πρόσβασης των βάσεων δεδομένων πρέπει να συμμορφώνονται με τα πρότυπα ασφάλειας της ΕΕΤΤ (όπως αυτά περιέχονται στην Πολιτική Ασφαλείας της ΕΕΤΤ) όσον αφορά τα χαρακτηριστικά τους, όπως το μήκος, την πολυπλοκότητα, το ιστορικό, το λεκτικό και την περίοδο ισχύος.

ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

12 Πρόσθετα θέματα ελέγχου πρόσβασης

12.1 Πρόσβαση σε κοινόχρηστο λογαριασμό

Μόνο εξουσιοδοτημένοι χρήστες πρέπει να έχουν πρόσβαση στους κοινόχρηστους λογαριασμούς της ΕΕΤΤ. Ο ηλεκτρονικός κατάλογος των χρηστών που είναι εξουσιοδοτημένοι για πρόσβαση στους κοινόχρηστους λογαριασμούς πρέπει να είναι πάντα διαθέσιμος και ενημερωμένος, να φυλάσσεται από τον Ιδιοκτήτη των Πληροφοριών και να υποβάλλεται σε τακτική αξιολόγηση από τον Υπεύθυνο Ασφάλειας Πληροφοριακών Συστημάτων της ΕΕΤΤ.

12.2 Έλεγχοι και ανάλυση κινδύνου

Στις περιπτώσεις που χρησιμοποιούνται κοινόχρηστοι λογαριασμοί στα πληροφοριακά συστήματα της ΕΕΤΤ, θα πρέπει να εφαρμόζονται αντισταθμιστικοί έλεγχοι για τον περιορισμό των σχετικών κινδύνων. Η επιλογή και η χρήση αυτών των ελέγχων πρέπει να εξετάζονται από την ΕΕΤΤ κατά τη διαδικασία ανάλυσης κινδύνων. Οποιοσδήποτε σχετικός έλεγχος χρησιμοποιείται, πρέπει να προσδιορίζεται και να αναγράφεται σε σχετικό κατάλογο.

12.3 Έλεγχος πρόσβασης στα αντίγραφα ασφαλείας

Η ΕΕΤΤ υλοποιεί κατάλληλα μέτρα για τον έλεγχο της φυσικής και λογικής πρόσβασης στα αντίγραφα ασφαλείας, σε αντιστοιχία με το σχήμα ταξινόμησης των πληροφοριακών πόρων.

13 Πρόσθετα θέματα ελέγχου απομακρυσμένης πρόσβασης

13.1 Απομακρυσμένη πρόσβαση εξωτερικών συνεργατών

Οι εξωτερικοί συνεργάτες με απομακρυσμένη πρόσβαση σε πόρους της ΕΕΤΤ (για σκοπούς διαχείρισης, για ανάπτυξη ή συντήρηση ή για οποιονδήποτε άλλο σκοπό) πρέπει να επικυρώνονται με τη χρήση ενός ισχυρού μηχανισμού επαλήθευσης ταυτότητας (π.χ. ταυτοποίησης με κωδικό μιας χρήσης (One-Time Password / OTP)[1] ή μέσω ειδοποίησης (push notification)[2]). Η διαδικασία σύνδεσης τρίτου μέρους στα συστήματα της ΕΕΤΤ αποτελεί αντικείμενο και παρουσιάζεται στην Πολιτική Διαχείρισης Τρίτων Μερών.

13.2 Αναθεώρηση δικαιωμάτων απομακρυσμένης πρόσβασης

Τα δικαιώματα των χρηστών για απομακρυσμένη πρόσβαση σε κρίσιμα ή ευαίσθητα πληροφοριακά συστήματα της ΕΕΤΤ πρέπει να ελέγχονται τουλάχιστον μία φορά το εξάμηνο.

---

[1] *One-Time Password ή OTP είναι ένας μοναδικός κωδικός πρόσβασης που ισχύει μόνο για μία περίοδο σύνδεσης ή συναλλαγή. Δηλαδή αλλάζει αυτόματα κάθε φορά που χρησιμοποιείται, σε αντίθεση με τους παραδοσιακούς κωδικούς πρόσβασης που παραμένουν στατικοί έως ότου αλλάξουν χειροκίνητα από το χρήστη.*

[2] *Push notification authentication είναι ο μηχανισμός που επαληθεύει την ταυτότητα ενός χρήστη στέλνοντας μια ειδοποίηση σε μια κινητή συσκευή, την οποία ο χρήστης μπορεί να εγκρίνει ή να αρνηθεί να παραχωρήσει πρόσβαση, παρακάμπτοντας την ανάγκη πληκτρολόγησης κωδικών πρόσβασης ή κωδικών μίας χρήσης.*

ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΤΑΧΥΔΡΟΜΕΙΩΝ

14 *Αλλαγές στην Πολιτική Διαχείρισης Λογικής Πρόσβασης*

Η ΕΕΤΤ αξιολογεί και επικαιροποιεί σε περιοδική βάση το σύνολο των πολιτικών και διαδικασιών που αφορούν στον έλεγχο πρόσβασης, ιδίως όταν λαμβάνουν χώρα σημαντικές αλλαγές στις λειτουργίες της ή στις τεχνολογικές εξελίξεις ή προκύπτουν μεταβολές στο περιβάλλον των κυβερνοαπειλών.

»

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 Λογικής Πρόσβασης*» πρέπει να εφαρμόζεται υποχρεωτικά και απαρέγκλιτα από το προσωπικό της ΕΕΤΤ.
4. **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 Διαχείρισης Λογικής Πρόσβασης»*.
    - Τροποποιεί την *«Πολιτική Διαχείρισης Λογικής Πρόσβασης»*, όποτε αυτό απαιτείται.

Ο ΠΡΟΕΔΡΟΣ

ΚΑΘΗΓΗΤΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ ΜΑΣΣΕΛΟΣ