ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΕΡΙΦΕΡΕΙΑ ΑΤΤΙΚΗΣ
ΠΕΡΙΦΕΡΕΙΑΚΟ ΣΥΜΒΟΥΛΙΟ
Γραφείο Προέδρου
Ταχ.Δ/νση : Λεωφ. Συγγρού 80-88
Ταχ. Κωδ. : 117 41 Αθήνα
Τηλ.: 213-2065244, 238, 518
e-mail : ssona@patt.gov.gr

ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΥΓΕΙΑ

Συνεδρίαση 12η

ΑΠΟΦΑΣΗ υπ' αριθμ. 106/2025

Σήμερα 30/5/2025, ημέρα Παρασκευή και ώρα 15:00, συνήλθαν σε τακτική συνεδρίαση τα μέλη του Περιφερειακού Συμβουλίου της Περιφέρειας Αττικής. Η συνεδρίαση πραγματοποιήθηκε, δια ζώσης, στην αίθουσα συνεδριάσεων του Δημοτικού Συμβουλίου του Δήμου Περάματος (*Ταχ. Δ/νση: Λεωφόρος Δημοκρατίας 28, Πέραμα (Δημαρχείο)*), κατά τις προβλέψεις των διατάξεων της παρ. 1 του άρθρου 167 του Ν. 3852/2010 (*ΦΕΚ 87/τ. Α'/07-6-2010*), όπως ισχύει, κατόπιν της υπ' αριθμ. πρωτ. 624937/23-5-2025 πρόσκλησης του Προέδρου κ. Βασίλειου Καπερνάρου, που κοινοποιήθηκε νόμιμα, στις 23/5/2025 στον Περιφερειάρχη Αττικής, σε καθένα από τους Αντιπεριφερειάρχες καθώς και σε καθένα από τους Περιφερειακούς Συμβούλους.

Θέμα 8ο Η.Δ.

Έγκριση Ενιαίας Πολιτικής Ασφαλείας Συστημάτων Πληροφορικής & Επικοινωνιών και Πολιτικής Ορθής Χρήσης Πληροφοριακών Συστημάτων, αρμοδιότητας της Διεύθυνσης Τεχνολογιών, Πληροφορικής & Επικοινωνιών (Τ.Π.Ε.) Περιφέρειας Αττικής (αρ. 32 του Οργανισμού Εσωτερικής Υπηρεσίας (Ο.Ε.Υ.) Περιφέρειας Αττικής, ΦΕΚ 1661/τ.Β'/2018).

Διαπιστώθηκε η απαρτία, κατά την έναρξη της συνεδρίασης, με σύνολο εξήντα δύο (62) παρόντων επί συνόλου ογδόντα πέντε (85) Περιφερειακών Συμβούλων, σύμφωνα με την υπ' αριθμ. 447/2023 απόφαση του Πολυμελούς Πρωτοδικείου Αθηνών, με την οποία επικυρώθηκε το αποτέλεσμα των εκλογών της 8ης Οκτωβρίου 2023 για την Περιφέρεια Αττικής και ανακηρύχθηκε ο επιτυχών και οι επιλαχόντες συνδυασμοί, ο Περιφερειάρχης και οι τακτικοί και αναπληρωματικοί περιφερειακοί σύμβουλοι κάθε συνδυασμού για την περιφερειακή περίοδο από 01-01- 2024 έως 31-12-2028, όπως αυτή διορθώθηκε με την υπ' αριθμ. 538/2023 όμοια και τροποποιήθηκε με την υπ'αριθμ. 186/2024 απόφαση του Διοικητικού Εφετείου Αθηνών.

Οι παρόντες και οι απόντες - μετά την αποχώρηση των παρόντων, κατά την έναρξη και έως πριν την ψηφοφορία επί του 1ου θέματος της ημερήσιας διάταξης, Περιφερειακών Συμβούλων της παράταξης «Αττικός Κύκλος Συνεργασίας & Εμπιστοσύνης- στη συζήτηση του συγκεκριμένου θέματος έχουν ως εξής:

Παρόντες:
Ο Περιφερειάρχης Αττικής κ. Χαρδαλιάς Νικόλαος
Τα μέλη του Περιφερειακού Συμβουλίου Αττικής:

Ο Πρόεδρος κ. Καπερνάρος Βασίλειος
Ο Γραμματέας κ. Μπενετάτος Στυλιανός

Η Αναπληρώτρια Περιφερειάρχης κ. Κεφαλογιάννη Χριστίνα

Οι Χωρικοί Αντιπεριφερειάρχες Αττικής κ.κ.: Αντωνάκου Σταυρούλα, Βαρελάς Κλεάνθης, Ζώμπος Κωνσταντίνος, Θεοδωρόπουλος Χρήστος, Καβαλλάρη Βασιλική (Βίκυ), Κεφαλογιάννη Λουκία, Λώλος Βασίλειος.

Οι Θεματικοί Αντιπεριφερειάρχες Αττικής κ.κ.: Αγγελάκη Δήμητρα, Αυγερινός Αθανάσιος (Θανάσης), Κοσμόπουλος Ελευθέριος, Μανωλάκος Λεωνίδας, Πάλλη - Γιαννακοπούλου Αλεξάνδρα, Σιάτρας Χαράλαμπος (Μπάμπης), Τουμαζάτου Μαριάννα.

Οι Περιφερειακοί Σύμβουλοι κ.κ.:
Αβραμίδης Γαβριήλ, Αβραμοπούλου Ελένη, Αδαμοπούλου Γεωργία (Τζίνα), Αλεξανδράτος Χαράλαμπος (Μπάμπης), Αλυμάρα Σοφία, Αντωνίου Άννα, Αργυράκη Βασιλεία (Μπέσσυ), Βαθιώτης Αθανάσιος, Βάρσου Μαργαρίτα, Βισκαδουράκης Αθανάσιος (Θανάσης), Βλάχος Γεώργιος, Βλάχου Γεωργία, Βοϊδονικόλας Σταύρος, Γαλακτόπουλος Πέτρος, Γεράκη Αικατερίνη, Δαμάσκος Δημήτριος, Καββαδίας Αντώνης, Κατσικάρης Δημήτριος, Κόκκαλης Βασίλειος, Κουρή Μαρία (Μαίρη), Κουτσογιαννόπουλος Θεόδωρος (Θοδωρής), Μαγκανάρης Νικόλαος, Μαρκουίζος (Ιαβέρης) Κωνσταντίνος, Μελάς Σταύρος, Μπαϊρακτάρης Πολυχρόνιος (Πολυχρόνης), Μπαρμπαγιάννη - Αδαμοπούλου Ευγενία, Παπαγεωργίου Νικόλαος, Παπασπύρου Αθανασία, Πετρόπουλος Βασίλειος, Πρωτούλης Ιωάννης, Ράπτης Ιωάννης, Σγουρός Ιωάννης, Συρίγος Βάλσαμος, Σφακιανάκης Εμμανουήλ (Μανώλης), Τάτσης Γεώργιος, Χιωτάκης Νικόλαος (Νίκος), Χρονοπούλου Νίκη.

Απόντες:
Τα μέλη του Περιφερειακού Συμβουλίου Αττικής:

Ο Αντιπρόεδρος κ. Κάβουρας Κωνσταντίνος.

Ο Χωρικός Αντιπεριφερειάρχης Αττικής κ. Βουτσινάς Ιωάννης.

Οι Θεματικοί Αντιπεριφερειάρχες Αττικής κ.κ.: Ασκητής Αθανάσιος (Θάνος), Γιακουμάτου Ευαγγελία (Εβίνα), Μιλλούση Βασιλική (Βίκυ), Πρεζεράκου Ευριδίκη (Έρρικα).

Οι Περιφερειακοί Σύμβουλοι κ.κ.:
Αγγέλης Σπυρίδων, Αλμπάνης Ευάγγελος, Αποστολίδου Κλεονίκη (Νίκη), Αυλωνίτου Χρυσάνθη, Γεωργιάδου Παρασκευή (Εύη), Γώγος Χρήστος, Ζαμπίδης Μιχαήλ (Άιρον Μάικ), Ιωακειμίδης Γεώργιος, Ιωακειμίδης Ευάγγελος, Καζάκου Μαρία, Καμπούρης Φίλιππος, Καραδήμα Ιωάννα, Κασίμης Χρήστος, Κατσούλης Αθανάσιος (Σάκης), Κοροβέση Μυρτώ, Κωνσταντέλλου Αθηνά, Λογοθέτη Αικατερίνη, Μακρή Σταυρούλα (Ρούλα), Μουζάλας Μάριος, Μπαλάφας Γεώργιος, Μωραϊτάκη Πικρού Ελευθερία (Ρίτα),

Ντούρος Γεώργιος, Ορφανός Αθανάσιος (Θάνος), Σχορτσανίτης Σοφοκλής, Τσουκαλάς Γεώργιος.

Χρέη υπηρεσιακών γραμματέων άσκησαν οι υπάλληλοι της Περιφέρειας Αττικής κ. Σωτηροπούλου Ευαγγελία και κ. Ζαλοκώστα Ευανθία- Αναστασία.

Ο Πρόεδρος του Περιφερειακού Συμβουλίου κ. Βασίλειος Καπερνάρος έδωσε το λόγο στην Αναπληρώτρια Περιφερειάρχη, κ. Χριστίνα Κεφαλογιάννη, η οποία έθεσε υπ' όψιν του Περιφερειακού Συμβουλίου την υπ' αριθμ. πρωτ. 596639/19-5-2025 εισήγηση της Δ/νσης Τεχνολογιών Πληροφορικής & Επικοινωνιών (ΤΠΕ) Περιφέρειας Αττικής, που εστάλη με την πρόσκληση και έχει ως εξής:

Έχοντας υπόψη:

1. *Τις διατάξεις του **Ν.3852/2010** «Νέα Αρχιτεκτονική της Αυτοδιοίκησης και της Αποκεντρωμένης Διοίκησης – Πρόγραμμα Καλλικράτης» (ΦΕΚ 87/Α/07-06-2010), όπως τροποποιήθηκε και ισχύει.*
2. *Τις διατάξεις του **Ν. 4071/2012** (ΦΕΚ 85/Α΄/11-04-2012) «Ρυθμίσεις για την τοπική ανάπτυξη, την αυτοδιοίκηση και την αποκεντρωμένη διοίκηση Ενσωμάτωση Οδηγίας 2009/50/ΕΚ», όπως τροποποιήθηκε και ισχύει.*
3. *Τις διατάξεις του Ν.4555/2018 (ΦΕΚ 133/Α' /19-07-2018) «Μεταρρύθμιση του θεσμικού πλαισίου της Τοπικής Αυτοδιοίκησης – εμβάθυνση της δημοκρατίας – ενίσχυση της συμμετοχής- βελτίωση της οικονομικής και αναπτυξιακής λειτουργίας των ΟΤΑ: ΠΡΟΓΡΑΜΜΑ ΚΛΕΙΣΘΕΝΗΣ».*
4. *Τις διατάξεις του **Ν. 3861/2010** (ΦΕΚ Α΄112/13-07-2010) «Ενίσχυση της διαφάνειας με την υποχρεωτική ανάρτηση νόμων και πράξεων των κυβερνητικών, διοικητικών και αυτοδιοικητικών οργάνων στο διαδίκτυο «Πρόγραμμα Διαύγεια» και άλλες διατάξεις».*
5. *Τις διατάξεις του **Ν. 4250/2014** (ΦΕΚ 74/τ.Α΄/26-03-2014) «Διοικητικές Απλουστεύσεις – Καταργήσεις, Συγχωνεύσεις Νομικών Προσώπων και Υπηρεσιών του Δημοσίου Τομέα – Τροποποίηση Διατάξεων του Π.Δ. 318/1992 (Α΄ 161) και λοιπές ρυθμίσεις.»*
6. *Τις διατάξεις του **Ν.2690/1999** (ΦΕΚ 45/Α'), άρθρο 14 του Κώδικα Διοικητικής Διαδικασίας.*
7. *Την υπ' αρ. 37419/13479/08-05-2018 (ΦΕΚ 1661/τ.Β΄/11-05-2018) Απόφαση του Συντονιστή Αποκεντρωμένης Διοίκησης Αττικής «Έγκριση της υπ' αρ. 121/2018 Απόφασης του Περιφερειακού Συμβουλίου Περιφέρειας Αττικής περί «Τροποποίησης-επικαιροποίησης του Οργανισμού Εσωτερικής Υπηρεσίας της Περιφέρειας Αττικής».*
8. *Την υπ. αριθ. **18641/05-01-2024** (ΑΔΑ: ΨΩ9Ζ7Λ7-ΜΧΥ) Απόφαση του Περιφερειάρχη Αττικής περί «Ορισμού Αναπληρώτριας Περιφερειάρχη και Αντιπεριφερειαρχών».*
9. *Την υπ. αριθ. **377330/07-04-2024** (ΦΕΚ 2121/τ. Β΄/07.04.2024) Απόφαση του Περιφερειάρχη Αττικής περί: «Μεταβίβασης αρμοδιοτήτων στον Αναπληρωτή Περιφερειάρχη, σε Αντιπεριφερειάρχες, σε Περιφερειακούς Συμβούλους και παροχή εξουσιοδότησης υπογραφής «Με εντολή Περιφερειάρχη» στον Εκτελεστικό Γραμματέα της Περιφέρειας Αττικής, στον Ειδικό Γραμματέα της Περιφέρειας Αττικής, σε Προϊσταμένους Γενικών Διευθύνσεων, Διευθύνσεων και Αυτοτελών Διευθύνσεων της Περιφέρειας Αττικής και σε Προϊσταμένους Τμημάτων της Γενικής Διεύθυνσης*

Εσωτερικής Λειτουργίας της Περιφέρειας Αττικής», όπως ισχύει.

10. *Τις διατάξεις του **Ν. 4070/2012** (ΦΕΚ 82/Α΄/10-04-2012) «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις».*
11. *Τις διατάξεις του **Ν. 4727/2020** (ΦΕΚ 184/Α') «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».*
12. *Το εγχειρίδιο κυβερνοασφάλειας της Εθνικής Αρχής Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης α.π. 17728/ΕΞ 2021/04-06-2021 «Βέλτιστες πρακτικές για την προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων».*
13. *Τις διατάξεις του **Ν. 5160/2024** (ΦΕΚ 195/Α'/27-11-2024) «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».*
14. *Τις διατάξεις του Ν. 4961/2022 (ΦΕΚ 146/Α'/27-7-2022) «Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις».*
15. *Την Κ.Υ.Α. υπ' αρ. **1689/2025** (ΦΕΚ 2186/Β'/06-05-2025) «Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων».*
16. *Το γεγονός ότι από την παρούσα δεν προκαλείται δαπάνη σε βάρος του κρατικού προϋπολογισμού.*
17. *Την ανάγκη καθορισμού ενιαίας πολιτικής ασφάλειας και πολιτικής ορθής χρήσης πληροφοριακών συστημάτων για την ολιστική προσέγγιση του κινδύνου (all hazards approach), που αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά που άπτονται της ασφάλειας τους.*

ΕΙΣΗΓΟΥΜΑΣΤΕ

Την έγκριση α) της Ενιαίας Πολιτικής Ασφαλείας Συστημάτων Πληροφορικής & Επικοινωνιών και β) της Πολιτικής Ορθής Χρήσης Πληροφοριακών Συστημάτων, αρμοδιότητας της Διεύθυνσης Τ.Π.Ε. (αρ. 32 του Ο.Ε.Υ., ΦΕΚ 1661/Β/2018).

Επισυνάπτονται τα κείμενα των πολιτικών.

(Τα συνημμένα κείμενα Πολιτικών της ανωτέρω εισήγησης επισυνάπτονται και αποτελούν αναπόσπαστο μέρος της παρούσας απόφασης.)

Το Περιφερειακό Συμβούλιο Αττικής
μετά από διαλογική συζήτηση μεταξύ των μελών του
και

λαμβάνοντας υπόψη:

- την ανάγκη καθορισμού ενιαίας πολιτικής ασφάλειας και πολιτικής ορθής χρήσης πληροφοριακών συστημάτων για την ολιστική προσέγγιση του κινδύνου (all hazards approach), που αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών

και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά που άπτονται της ασφάλειας τους,

- την ανωτέρω εισήγηση της Δ/νσης Τεχνολογιών Πληροφορικής & Επικοινωνιών (ΤΠΕ) Περιφέρειας Αττικής,

αποφασίζει ομόφωνα

Την έγκριση:

Α) της Ενιαίας Πολιτικής Ασφαλείας Συστημάτων Πληροφορικής & Επικοινωνιών, όπως επισυνάπτεται και αποτελεί αναπόσπαστο μέρος της παρούσης και

Β) της Πολιτικής Ορθής Χρήσης Πληροφοριακών Συστημάτων, όπως επισυνάπτεται και αποτελεί αναπόσπαστο μέρος της παρούσης,

αρμοδιότητας της Δ/νσης Τεχνολογιών, Πληροφορικής & Επικοινωνιών (Τ.Π.Ε.) Περιφέρειας Αττικής (αρ. 32 του Οργανισμού Εσωτερικής Υπηρεσίας (Ο.Ε.Υ.) Περιφέρειας Αττικής, ΦΕΚ 1661/τ.Β'/2018).

Απείχαν της ψηφοφορίας οι Περιφερειακοί Σύμβουλοι της παράταξης «ΛΑΪΚΗ ΣΥΣΠΕΙΡΩΣΗ ΑΤΤΙΚΗΣ» κ.κ.: Ι. Πρωτούλης, Αικ. Γεράκη, Α. Καββαδίας, Στ. Μπενετάτος, Β. Πετρόπουλος, Β. Συρίγος, Γ. Τάτσης, Ν. Χρονοπούλου.

Ο ΠΡΟΕΔΡΟΣ ΤΟΥ Π.Σ.	**Ο ΓΡΑΜΜΑΤΕΑΣ ΤΟΥ Π.Σ.**
ΒΑΣΙΛΕΙΟΣ ΚΑΠΕΡΝΑΡΟΣ	**ΣΤΥΛΙΑΝΟΣ ΜΠΕΝΕΤΑΤΟΣ**

ΑΔΑ: Ψ6Λ37Λ7-ΩΞ2

@ΣΗΔΕ ΙΡΙΔΑ
682afd823e7c231e23f4decb
ΑΠ:596639
Υπογραφή: 19/05/25 13:55
Διανομή: 19/05/25 13:56

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΠΕΡΙΦΕΡΕΙΑ ΑΤΤΙΚΗΣ

ΕΝΙΑΙΑ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΕΠΙΚΟΙΝΩΝΙΩΝ

ΜΑΙΟΣ 2025

Πίνακας περιεχομένων

Πίνακας περιεχομένων

1. ΕΙΣΑΓΩΓΗ

Το παρόν έγγραφο αποτελεί την Πολιτική Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών της Περιφέρειας Αττικής που διαχειρίζονται και υποστηρίζονται από την Διεύθυνση Τεχνολογιών Πληροφορικής και Επικοινωνιών (Τ.Π.Ε.): αρ. 32 του Ο.Ε.Υ. (ΦΕΚ 1661/Β/2018), και καθορίζει τον τρόπο προστασίας των συστημάτων πληροφορικής και επικοινωνιών από απειλές, διαρροές και μη εξουσιοδοτημένη πρόσβαση. Επίσης η πολιτική αυτή καθορίζει τις αρχές, τις διαδικασίες και τις ευθύνες για την προστασία από κυβερνοαπειλές και την αντιμετώπιση περιστατικών ασφαλείας.

2. ΣΚΟΠΟΣ - ΠΡΟΣΕΓΓΙΣΗ ΔΙΑΧΕΙΡΙΣΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

2.1 ΣΚΟΠΟΣ – ΣΤΟΧΟΙ

Η παρούσα πολιτική καθορίζει τα απαραίτητα μέτρα για την προστασία των πληροφοριακών συστημάτων, των δεδομένων του οργανισμού και την ενίσχυση της κυβερνοασφάλειας.

Οι βασικοί στόχοι της πολιτικής ασφάλειας του Φορέα είναι:

- **Προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων**.
  - ✓ Διαθεσιμότητα: Διασφάλιση ότι τα συστήματα, τα δεδομένα και οι υπηρεσίες είναι διαθέσιμα όταν χρειάζονται.
  - ✓ Ακεραιότητα: Προστασία των δεδομένων και των συστημάτων από μη εξουσιοδοτημένες τροποποιήσεις ή καταστροφές.
  - ✓ Εμπιστευτικότητα: Διασφάλιση ότι τα δεδομένα και οι πληροφορίες είναι προσβάσιμα μόνο από εξουσιοδοτημένα άτομα ή συστήματα.
- **Προετοιμασία για Κυβερνοαπειλές.**
  - ✓ Εφαρμογή μέτρων που αποτρέπουν – ελαχιστοποιούν την τρωτότητα των πληροφοριακών συστημάτων του Φορέα έναντι κυβερνοεπιθέσεων ή περιστατικών ασφαλείας.

- ✓ Εφαρμογή μέτρων που περιορίζουν το αντίκτυπο μιας επίθεσης.
- ✓ Δημιουργία και εφαρμογή διαδικασιών για επιχειρησιακή συνέχεια, ώστε ο Φορέας να μπορεί να ανακάμψει γρήγορα και στο μέγιστο δυνατό βαθμό από περιστατικά ασφαλείας.

- **Συμμόρφωση με Νομοθεσία – Κανονισμούς**.

Διασφάλιση ότι η πολιτική ασφαλείας συμμορφώνεται με τις ισχύουσες νομοθετικές διατάξεις. Η συμμόρφωση περιλαμβάνει:

- ✓ Την εφαρμογή τεχνικών και οργανωτικών μέτρων ασφαλείας.
- ✓ Την αναφορά σοβαρών περιστατικών στις αρμόδιες αρχές εντός προκαθορισμένων χρονικών ορίων.
- ✓ Την τακτική αναθεώρηση και ενημέρωση των πολιτικών και των διαδικασιών.

2.2 ΠΡΟΣΕΓΓΙΣΗ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ

Η παρούσα πολιτική για να δημιουργήσει μια ολοκληρωμένη προσέγγιση διαχείρισης ασφάλειας για την προστασία των χρηστών, των συστημάτων και των δεδομένων της Περιφέρειας Αττικής, συνδυάζει τα παρακάτω στοιχεία:

- **Ανάλυση Κινδύνων:** Τακτική αξιολόγηση των κινδύνων για τα πληροφοριακά συστήματα και τις πληροφορίες.
  - Ταυτοποίηση πιθανών κινδύνων και απειλών.
  - Εκτίμηση της πιθανότητας και των επιπτώσεων αυτών των κινδύνων.
  - Καθορισμός προτεραιοτήτων για την αντιμετώπιση των κινδύνων.
- **Προληπτικά Μέτρα:**
  - Εφαρμογή μέτρων για την πρόληψη, τον εντοπισμό και την αντιμετώπιση των κινδύνων.
  - Χρήση τεχνολογιών και συστημάτων που μειώνουν τον κίνδυνο.
- **Ετοιμότητα και Αντιμετώπιση Συμβάντων:**
  - Ανάπτυξη σχεδίων αντιμετώπισης έκτακτων αναγκών.
  - Εκπαίδευση και ενημέρωση του προσωπικού για την αντιμετώπιση κρίσεων.
  - Δημιουργία συστημάτων παρακολούθησης και ειδοποίησης.

- **Συνεχής Εποπτεία και Αξιολόγηση:**
    - Παρακολούθηση και αξιολόγηση της αποτελεσματικότητας των μέτρων ασφάλειας.
    - Τροποποίηση και βελτίωση των πολιτικών και διαδικασιών με βάση τα αποτελέσματα.
- **Εκπαίδευση και Ευαισθητοποίηση:**
    - Εκπαίδευση των εργαζομένων και των ενδιαφερομένων μερών σε θέματα ασφάλειας.
    - Ευαισθητοποίηση για την σημασία της συμμόρφωσης με τις πολιτικές ασφάλειας.
- **Νομοθετικό και Κανονιστικό Πλαίσιο:**
    - Συμμόρφωση με τους νόμους, τους κανονισμούς και τα πρότυπα που αφορούν την κυβερνοασφάλεια.
    - Τήρηση των κατευθυντήριων γραμμών και των βέλτιστων πρακτικών του κλάδου.

2.3 ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η ισχύς της παρούσας πολιτικής είναι καθολική και συγκεκριμένα ισχύει για:

- Όλα τα πληροφοριακά συστήματα, δίκτυα, εφαρμογές και δεδομένα που υποστηρίζει και διαχειρίζεται η Διεύθυνση Τ.Π.Ε., ανεξάρτητα από τη φυσική ή ψηφιακή τους θέση.
- Όλους τους υπαλλήλους, συνεργάτες, παρόχους και τρίτους που έχουν πρόσβαση στα παραπάνω συστήματα και τα δεδομένα τους.

2.4 ΕΥΘΥΝΕΣ ΚΑΙ ΡΟΛΟΙ

Για την αποτελεσματική εφαρμογή της παρούσας πολιτικής, καθορίζονται οι ακόλουθοι ρόλοι και ευθύνες:

- **Διοίκηση Περιφέρειας**: Ευθύνεται για την έγκριση της πολιτικής ασφαλείας, την κατανομή των απαραίτητων πόρων και την επίβλεψη-υποστήριξη της συνολικής

εφαρμογής της. Εκπαιδεύεται σε θέματα κυβερνοασφάλειας και διασφαλίζει την εκπαίδευση όλων των υπαλλήλων του Φορέα.

- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.)**: Παρακολουθεί και συντονίζει την εφαρμογή της πολιτικής ασφάλειας, διαχειρίζεται κινδύνους και αναφέρει περιστατικά στις αρμόδιες αρχές.
- **Δ/νση Τεχνολογιών Πληροφορικής & Επικοινωνιών (Τ.Π.Ε.)**: Εφαρμόζει τα τεχνικά μέτρα ασφάλειας και είναι υπεύθυνη για τη διαχείριση και τη συντήρηση των υποδομών ασφάλειας.
- **Υπεύθυνος Προστασίας Δεδομένων (DPO - Data Protection Officer)**: Υπεύθυνος για θέματα που εμπίπτουν στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR).
- **Υπάλληλοι-Χρήστες**: Οφείλουν να τηρούν τις πολιτικές, τους κανονισμούς, τις διαδικασίες ασφάλειας που έχει θεσπίσει ο Φορέας και τις οδηγίες που τους κοινοποιούνται. Επιπρόσθετα οφείλουν να αναφέρουν άμεσα κάθε πιθανό περιστατικό κυβερνοασφάλειας που υποπίπτει στην αντίληψή τους. Τέλος είναι υποχρεωμένοι να συμμετέχουν σε σχετικά προγράμματα εκπαίδευσης.

3. ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Η Ανάλυση Κινδύνων Πληροφοριακών Συστημάτων είναι μια κρίσιμη διαδικασία που στόχο έχει να αναγνωρίσει τους κινδύνους που αντιμετωπίζουν τα πληροφοριακά συστήματα του Φορέα και να τους αξιολογήσει ως προς τη σοβαρότητά τους. Αποτέλεσμα αυτής της διαδικασίας, είναι ο καθορισμός των προτεραιοτήτων και το κατάλληλο σχέδιο για την αποτελεσματική αντιμετώπιση των κινδύνων.

3.1 ΚΑΘΟΡΙΣΜΟΣ ΠΕΔΙΟΥ ΕΦΑΡΜΟΓΗΣ

Προσδιορισμός των συστημάτων και των πληροφοριών: Καθορίζονται με σαφήνεια τα πληροφοριακά συστήματα, οι εφαρμογές, οι υποδομές επικοινωνιών και τα δεδομένα του Φορέα που θα συμπεριληφθούν στην ανάλυση κινδύνου. Συγκεκριμένα:

- ✓ Υλικό (Hardware): Εξυπηρετητές, υπολογιστές, δικτυακός και τηλεπικοινωνιακός εξοπλισμός, αποθηκευτικά μέσα.
- ✓ Λογισμικό (Software): Λειτουργικά συστήματα, εφαρμογές, βάσεις δεδομένων, εργαλεία διαχείρισης.
- ✓ Δεδομένα: Ευαίσθητα και μη ευαίσθητα δεδομένα, ηλεκτρονικά αρχεία, στοιχεία τηλεπικοινωνιών.
- ✓ Ανθρώπινο Δυναμικό:
  - Χρήστες, διαχειριστές και τεχνικό προσωπικό του Φορέα.
  - Εξωτερικοί συνεργάτες και προμηθευτές που παρέχουν υπηρεσίες σχετικές με την τεχνολογία και την ασφάλεια πληροφοριών.
- ✓ Διαδικασίες και Πολιτικές: Οδηγίες λειτουργίας, επιμέρους πολιτικές ασφαλείας και πρωτόκολλα ανταπόκρισης.

- Καθορισμός των στόχων: Ορίζονται οι στόχοι της ανάλυσης κινδύνου, όπως η προστασία από συγκεκριμένες απειλές, ή η συμμόρφωση με κανονισμούς. Η ανάλυση κινδύνων πληροφοριακών συστημάτων στοχεύει στην αναγνώριση, αξιολόγηση και αντιμετώπιση πιθανών απειλών που θα μπορούσαν να επηρεάσουν τη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα των πληροφοριών του Φορέα.

3.2 ΑΝΑΓΝΩΡΙΣΗ ΑΠΕΙΛΩΝ

Αναγνωρίζονται και καταγράφονται οι πιθανές απειλές που μπορεί να επηρεάσουν τα πληροφοριακά συστήματα και τα δεδομένα τους, όπως:

- ✓ Φυσικές Απειλές: Φωτιά, πλημμύρα, σεισμός.
- ✓ Τεχνικές Απειλές: Αστοχίες εξοπλισμού, διακοπές ρεύματος.
- ✓ Κυβερνοαπειλές: Επιθέσεις malware, hacking, phishing.
- ✓ Ανθρωπογενείς Απειλές: Ανθρώπινα λάθη, εσωτερικές διαρροές, κακόβουλες ενέργειες.

3.3 ΑΝΑΓΝΩΡΙΣΗ ΕΥΠΑΘΕΙΩΝ

Αναγνωρίζονται και καταγράφονται οι ευπάθειες και τα σημεία αδυναμίας που μπορούν να εκμεταλλευτούν οι απειλές. Διενεργούνται έλεγχοι ευπάθειας (vulnerability assessment) για τον εντοπισμό αδυναμιών στα συστήματα και τις εφαρμογές. Αυτές μπορεί να περιλαμβάνουν:

- ✓ Τεχνικές Ευπάθειες: Παρωχημένο λογισμικό, αδύναμοι κωδικοί, κακή διαχείριση ενημερώσεων.
- ✓ Διοικητικές Ευπάθειες: Έλλειψη πολιτικών ασφαλείας, ανεπάρκεια ελέγχου πρόσβασης.
- ✓ Φυσικές Ευπάθειες: Ανεπαρκής φυσική προστασία του εξοπλισμού.

3.4 ΕΚΤΙΜΗΣΗ ΚΙΝΔΥΝΟΥ

Προσδιορίζεται η πιθανή επίπτωση που μπορεί να επιφέρει ένα περιστατικό ασφαλείας. Λαμβάνεται υπόψη:

- Συνδυασμός πιθανότητας και επίπτωσης: Ο συνδυασμός της πιθανότητας εμφάνισης κάθε απειλής με τη σοβαρότητα των επιπτώσεων, δίνει το βαθμό εκτίμησης κινδύνου και την κατηγοριοποίησή του σε Low Risk, Medium Risk, High Risk, Critical Risk.
- Μεθοδολογίες: Χρησιμοποίηση μεθοδολογιών ανάλυσης κινδύνου, όπως η μέθοδος NIST. Τα σημεία ελέγχου εντάσσονται στην κατηγοριοποίηση που είναι σύμφωνη με

το πλαίσιο ελέγχου NIST, σύμφωνα με το οποίο γίνεται διαχωρισμός σε πέντε (5) λειτουργικές ενότητες (Identify, Protect, Detect, Respond, Recover).

3.5 ΑΝΑΠΤΥΞΗ ΣΧΕΔΙΟΥ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΩΝ ΚΙΝΔΥΝΩΝ

Σε συνέχεια της εκτίμησης των κινδύνων προτείνονται μέτρα ασφάλειας για την αντιμετώπιση των κινδύνων, όπως:

- Μέτρα ασφάλειας:
  - ✓ Τεχνικά Μέτρα: next generation firewalls-utm, ενημερώσεις λογισμικού, κρυπτογράφηση δεδομένων.
  - ✓ Διοικητικά Μέτρα: Εκπαίδευση προσωπικού, πολιτικές πρόσβασης.
  - ✓ Φυσικά Μέτρα: Έλεγχος φυσικής πρόσβασης, κάμερες ασφαλείας.
- Προτεραιοποίηση: Τα μέτρα ασφάλειας σχεδιάζονται με προτεραιότητα σε εκείνα που μειώνουν τους σημαντικότερους και πιο άμεσους κινδύνους.

3.6 ΤΕΚΜΗΡΙΩΣΗ ΚΑΙ ΑΝΑΦΟΡΑ

Η τεκμηρίωση της ανάλυσης κινδύνου περιλαμβάνει:

- ✓ Αναφορές για τη διοίκηση.
- ✓ Τεκμηρίωση των ληφθέντων μέτρων.
- ✓ Αρχείο δοκιμών και αξιολογήσεων.

3.7 ΣΥΝΕΧΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΚΑΙ ΑΝΑΘΕΩΡΗΣΗ

Η ανάλυση κινδύνου είναι μια συνεχής διαδικασία. Περιλαμβάνει:

- ✓ Παρακολούθηση νέων απειλών και ευπαθειών.
- ✓ Αναθεώρηση των μέτρων ασφαλείας.
- ✓ Βελτιστοποίηση των διαδικασιών προστασίας.

4. ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Ακολουθούν τα τεχνικά μέτρα ασφάλειας πληροφοριακών συστημάτων.

4.1 ΚΑΤΑΓΡΑΦΗ ΥΛΙΚΟΥ ΚΑΙ ΛΟΓΙΣΜΙΚΟΥ

Ο Φορέας διατηρεί πλήρη και επικαιροποιημένο κατάλογο των πόρων που φιλοξενούνται είτε στην φυσική υποδομή του, είτε σε cloud περιβάλλον. Περιλαμβάνονται:

- ✓ Υλικό (Hardware): Εξυπηρετητές, υπολογιστές, δικτυακός εξοπλισμός, φορητές ηλεκτρονικές συσκευές, αποθηκευτικά μέσα.
- ✓ Λογισμικό (Software): Λειτουργικά συστήματα, εφαρμογές, βάσεις δεδομένων, εργαλεία διαχείρισης.

Στον Φορέα υπάρχει εφαρμογή στην οποία είναι καταγεγραμμένος ο εξοπλισμός και τα συστήματα της Περιφέρειας Αττικής και επικαιροποιείται ανά τακτά χρονικά διαστήματα.

4.2 ΑΣΦΑΛΗΣ ΔΙΑΜΟΡΦΩΣΗ ΕΞΟΠΛΙΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ

Υλοποιείται ασφαλής διαμόρφωση σε σταθμούς εργασίας (σταθεροί και φορητοί), διακομιστές, δικτυακές συσκευές (δρομολογητές, μεταγωγείς, firewalls) και εφαρμογές ως εξής:

- Εφαρμόζονται οι βασικές ρυθμίσεις ασφάλειας για τα λειτουργικά συστήματα όλων των υπολογιστών, διακομιστών και δικτυακών συσκευών.
  - ✓ Ισχυροί Κωδικοί Πρόσβασης: Χρήση πολύπλοκων κωδικών (τουλάχιστον 12 χαρακτήρες με αριθμούς, γράμματα και σύμβολα).
  - ✓ Αρχή Ελάχιστων Δικαιωμάτων (Least Privilege Access): Χρήστες και υπηρεσίες έχουν μόνο τα απαραίτητα δικαιώματα.
  - ✓ Τοπικό Προφίλ Διαχειριστών: Αποφυγή χρήσης λογαριασμού διαχειριστή (administrator) για καθημερινές εργασίες.
- Εφαρμόζονται οι ενημερώσεις ασφάλειας (security patches) σε λειτουργικά συστήματα και εφαρμογές.

- Αλλαγή του προεπιλεγμένου κωδικού πρόσβασης (default password) σε κάθε νέο προϊόν κατά την εγκατάστασή του.
- Διαχείριση συστημάτων και εφαρμογών στα οποία έχει λήξει η υποστήριξη από τον κατασκευαστή λαμβάνοντας υπόψη τις διαδικασίες αποκλίσεων και εξαιρέσεων.

4.3 ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ ΚΑΙ ΥΠΟΔΟΜΩΝ

Ο Φορέας λαμβάνει κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των δικτυακών του υποδομών, σύμφωνα με την ισχύουσα νομοθεσία και τις βέλτιστες πρακτικές. Τα βασικά στοιχεία που διέπουν την ασφάλεια του δικτύου και των υποδομών είναι:

- Χρήση συσκευών ενοποιημένης αντιμετώπισης απειλών (UTMs): Εγκατάσταση και παραμετροποίηση για τον έλεγχο εισερχόμενης και εξερχόμενης κυκλοφορίας δικτύου.
- Περιορισμός πρόσβασης στο διαδίκτυο και εφαρμογές (Web Filtering & Content Control): Αποτροπή πρόσβασης σε κακόβουλους, ή μη εγκεκριμένους ιστότοπους.
- DDoS Protection: Εφαρμογή μηχανισμών προστασίας έναντι κατανεμημένων επιθέσεων άρνησης υπηρεσίας.
- Συστήματα Ανίχνευσης και Πρόληψης Εισβολών (IDS/IPS): Υλοποιείται ανίχνευση και αποτροπή μη εξουσιοδοτημένης πρόσβασης.
- Διαχωρισμός δικτύων (Network Segmentation): Διαχωρισμός κρίσιμων υπηρεσιών από τα υπόλοιπα εταιρικά ή δημόσια δίκτυα. Ο γενικός κανόνας είναι ένα υποδίκτυο του δικτύου «ΣΥΖΕΥΞΙΣ» ανά κτίριο, ενώ μέρος της τμηματοποίησης του δικτύου υλοποιείται με VLANs.
- VPN και Ασφαλείς Απομακρυσμένες Συνδέσεις:
    - ✓ Υποχρεωτική χρήση VPN για απομακρυσμένη πρόσβαση. Η απομακρυσμένη πρόσβαση σε κρίσιμα συστήματα και εφαρμογές επιτρέπεται μόνο μέσω ασφαλών καναλιών με ταυτοποίηση/αυθεντικοποίηση και κρυπτογράφηση (VPN). Κατά τη σύνδεση μέσω VPN γίνεται χρήση αυθεντικοποίησης πολλαπλών παραγόντων (Multiple Factor Authentication – MFA).

- ✓ Αποστολή αναλυτικών οδηγιών στους εργαζόμενους για την ασφαλή διαμόρφωση του οικιακού υπολογιστικού και δικτυακού εξοπλισμού τους.
- ✓ Επικαιροποίηση της λίστας των δικαιούχων πρόσβασης μέσω VPN.

- Ασφάλεια Wi-Fi: Τα ασύρματα δίκτυα του Φορέα προστατεύονται με ισχυρή πιστοποίηση και διαχωρισμό μεταξύ επισκεπτών και εσωτερικών χρηστών. Παρέχουν στους χρήστες πρόσβαση στο διαδίκτυο και διαχωρίζονται από το εσωτερικό τοπικό δίκτυο είτε λογικά είτε φυσικά.
- Πολιτικές Ενημερώσεων Δικτυακών Συσκευών (Patch Management): Ενημέρωση δικτυακού εξοπλισμού για προστασία από ευπάθειες.

4.4 ΤΗΡΗΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ ΣΥΜΒΑΝΤΩΝ

Συλλογή και ανάλυση των αρχείων καταγραφής συμβάντων από το σύνολο του εξοπλισμού, για την έγκαιρη ανίχνευση και αντιμετώπιση περιστατικών.

- Ενεργοποίηση της καταγραφής logs σε κάθε σταθμό εργασίας, server και δικτυακή συσκευή.
- Σύστημα Κεντρικής Παρακολούθησης και Ανάλυσης Συμβάντων (SIEM): Όλα τα κρίσιμα συστήματα και δικτυακές συσκευές αποστέλλουν καταγραφές (logs) σε σύστημα SIEM, το οποίο εντοπίζει ύποπτα μοτίβα και παρέχει αναφορές και ειδοποιήσεις ασφαλείας.

4.5 ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

Ο Φορέας εφαρμόζει μια σειρά από τεχνικά και οργανωτικά μέτρα για την πρόληψη, ανίχνευση και εξουδετέρωση κακόβουλου λογισμικού (malware) σε όλα τα συστήματα και τις υποδομές του.

Τα βασικά μέτρα που ακολουθούνται περιλαμβάνουν:

- Αυτόματη σάρωση και ανάλυση ύποπτων αρχείων και εφαρμογών (Antivirus, Anti-Malware) μέσω κεντρικοποιημένου λογισμικού διαδικτυακής ασφάλειας για την προστασία από κακόβουλο λογισμικό όλων των υπολογιστών, (προσωπικών υπολογιστών και εξυπηρετητών) και διαθέτουν τις πλέον πρόσφατες ενημερώσεις.

- Χρήση συστημάτων ανίχνευσης και αποτροπής κακόβουλου λογισμικού σε δίκτυα και endpoints (EDR – Endpoint Detection and Response).
- Τακτική ενημέρωση λειτουργικών συστημάτων και λογισμικών για αποτροπή εκμετάλλευσης ευπαθειών.
- Χρήση Application Whitelisting για την αποτροπή μη εξουσιοδοτημένων εφαρμογών.
- Εφαρμογή ελέγχων USB και αφαιρούμενων μέσων, για αποφυγή μόλυνσης από εξωτερικές συσκευές.
- Ενημέρωση και ευαισθητοποίηση προσωπικού για την αναγνώριση κινδύνων και απειλών μέσω ορθών πρακτικών κυβερνοϋγιεινής.

4.6 ΔΙΑΧΕΙΡΙΣΗ ΤΑΥΤΟΤΗΤΑΣ ΚΑΙ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ

Η προστασία των πληροφοριακών πόρων του Φορέα επιτυγχάνεται μέσω αυστηρής διαχείρισης ταυτότητας και ελέγχου της πρόσβασης σε κρίσιμα συστήματα και δεδομένα. Στόχος είναι να διασφαλιστεί ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε συγκεκριμένους πόρους και υπηρεσίες, περιορίζοντας τον κίνδυνο από μη εξουσιοδοτημένη πρόσβαση και κακόβουλες ενέργειες.

Σε αυτό το τμήμα τα τεχνικά μέτρα περιλαμβάνουν:

- Πολιτική ελάχιστων δικαιωμάτων πρόσβασης (Least Privilege Access): Κάθε χρήστης, ανεξαρτήτως του ρόλου του, έχει πρόσβαση μόνο στα απολύτως απαραίτητα δεδομένα και συστήματα που απαιτούνται για την εκτέλεση των καθηκόντων του. Η πολιτική αυτή περιορίζει τα δικαιώματα πρόσβασης στο ελάχιστο δυνατό, μειώνοντας τον κίνδυνο εκμετάλλευσης κακόβουλων ενεργειών ή σφαλμάτων. Στους υπολογιστές του προσωπικού επιτρέπεται η σύνδεση με διαχειριστικούς λογαριασμούς μόνο στο αρμόδιο προσωπικό διαχείρισης. Οι εργαζόμενοι συνδέονται μόνο με δικαιώματα απλού χρήστη και χωρίς δυνατότητες ενεργειών που μπορεί να επηρεάσουν την συνολική λειτουργία και διαμόρφωση π.χ. απενεργοποίηση αντιικών προγραμμάτων, εγκατάσταση νέων προγραμμάτων ή αλλαγή ρυθμίσεων υπαρχόντων κ.λπ. Στους υπολογιστές αυτούς γίνεται από το αρμόδιο προσωπικό περιοδικός έλεγχος του εγκατεστημένου λογισμικού για τον

τυχόν εντοπισμό προγραμμάτων που δεν έχουν εγκατασταθεί με βάση εγκεκριμένες διαδικασίες. Ιδιαίτερη προσοχή δίνεται στις περιπτώσεις που συγκεκριμένες εφαρμογές έχουν σαν προϋπόθεση για την λειτουργία τους επαυξημένα δικαιώματα χρήστη (security-by-design).

- Διαχείριση κωδικών πρόσβασης: Μέσω της Υπηρεσίας Καταλόγου (Active Directory - AD) του Φορέα υπάρχει κεντρική διαχείριση ταυτοτήτων και προσβάσεων και συνδέεται με τους επιμέρους μηχανισμούς ταυτοποίησης των χρηστών στις εφαρμογές και τα συστήματα (π.χ. LDAP). Όπου αυτό δεν είναι εφικτό στο σύνολό του ή σε μέρος του, οι χρήστες είναι αποκλειστικά υπεύθυνοι να συμμορφώνονται με τις βέλτιστες πρακτικές που επιβάλλει η πολιτική συνθηματικών.

  Η πολιτική διαχείρισης των συνθηματικών των χρηστών, περιλαμβάνει κανόνες αποδοχής για το ελάχιστο μήκος και τους επιτρεπτούς χαρακτήρες των συνθηματικών (πολυπλοκότητα συνθηματικού), την ιστορικότητα του συνθηματικού και τη συχνότητα αλλαγής του.

  Η ίδια πολιτική συνθηματικών ακολουθείται στους κωδικούς πρόσβασης διαχειριστών και χρηστών στους προσωπικούς υπολογιστές (σταθερούς, φορητούς), tablets και στις άλλες συσκευές.

- Πολυπαραγοντικός έλεγχος ταυτότητας (MFA): Για την ενίσχυση της ασφάλειας ο Φορέας δύναται να υλοποιήσει πολυπαραγοντική ταυτοποίηση (MFA) όπου απαιτείται, για την πρόσβαση σε κρίσιμα συστήματα και εφαρμογές (π.χ. απομακρυσμένη πρόσβαση μέσω VPN), όπως κωδικός πρόσβασης και κωδικός από κινητή συσκευή ή βιομετρική ταυτοποίηση.
- Καταγραφή και ανάλυση δραστηριοτήτων πρόσβασης για εντοπισμό ανωμαλιών.
- Ενοποίηση ταυτοτήτων σε διαφορετικά συστήματα μέσω κεντρικών καταλόγων.
- Αδρανοποιημένος υπολογιστής: Προς αποφυγή μη εξουσιοδοτημένης πρόσβασης πρέπει να κλειδώνεται η χρήση του υπολογιστή, ο οποίος μένει χωρίς επίβλεψη, έστω και για μικρό χρονικό διάστημα, και να απαιτείται η εκ νέου ταυτοποίηση του χρήστη.

4.7 ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Καθορίζει τους κανόνες για τον έλεγχο πρόσβασης σε ευαίσθητα δεδομένα.

4.7.1 ΕΠΕΞΕΡΓΑΣΙΑ ΕΥΑΙΣΘΗΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Όσοι επεξεργάζονται ευαίσθητα προσωπικά δεδομένα και τα αποθηκεύουν σε ηλεκτρονικά μέσα του Φορέα, οφείλουν να ενημερώνουν την Διεύθυνση Τ.Π.Ε., η οποία θα προβαίνει στην υλοποίηση κατάλληλων τεχνικών μέτρων κρυπτογραφίας για τα εν λόγω δεδομένα.

4.7.2 ΠΡΩΤΟΚΟΛΛΑ ΔΙΑΔΙΚΤΥΟΥ

Εφαρμόζονται ασφαλή πρωτόκολλα επικοινωνίας μέσω διαδικτύου, όπως HTTPS, SFTP, SSH, SMTPS, IMAPS. Τα πληροφοριακά συστήματα και οι εφαρμογές με διεπαφή παγκόσμιου ιστού (web interfaces) πρέπει να λειτουργούν αποκλειστικά μέσω ασφαλούς (κρυπτογραφημένου) καναλιού (SSL/HTTPS), καθώς επίσης και οι ιστοσελίδες που περιλαμβάνουν φόρμες υποβολής προσωπικών δεδομένων.

Η πρόσβαση σε συγκεκριμένες υπηρεσίες και εφαρμογές του Διαδικτύου από το εσωτερικό δίκτυο του Φορέα (π.χ. μέσα κοινωνικής δικτύωσης, πλατφόρμες πολυμέσων) μπορεί να περιοριστεί ή και να απαγορευτεί μέσω των μηχανισμών και συστημάτων ασφάλειας.

4.7.3 ΚΑΛΕΣ ΠΡΑΚΤΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Η χρήση κρυπτογραφικών προγραμμάτων προτείνεται στις περιπτώσεις:

- στην ηλεκτρονική αποθήκευση κωδικών πρόσβασης
- στην αποστολή συνημμένων αρχείων που περιέχουν ευαίσθητες πληροφορίες (π.χ. προσωπικά δεδομένα) μέσω email
- στους σκληρούς δίσκους των φορητών υπολογιστών ώστε να ελαχιστοποιείται ο κίνδυνος διαρροής πληροφοριών ή μη εξουσιοδοτημένης πρόσβασης σε περίπτωση κλοπής ή απώλειας της συσκευής.

4.8 ΕΛΕΓΧΟΙ ΑΣΦΑΛΕΙΑΣ

Πραγματοποιούνται έλεγχοι αξιολόγησης των τεχνικών και οργανωτικών μέτρων προστασίας των πληροφοριακών συστημάτων του Φορέα. Συγκεκριμένα, διενεργούνται έλεγχοι ευπαθειών (vulnerability assessments) και δοκιμές παρείσδυσης (penetration testing) σύμφωνα με τις κείμενες διατάξεις, τον ισχύοντα κάθε φορά κίνδυνο από κυβερνοαπειλές και τις υπηρεσιακές ανάγκες του Φορέα.

5. ΔΙΑΔΙΚΑΣΙΑ ΛΗΨΗΣ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ

Η διαδικασία λήψης αντιγράφων ασφαλείας (backup) είναι θεμελιώδες μέτρο ασφάλειας για τη διατήρηση της ακεραιότητας και της διαθεσιμότητας των δεδομένων του οργανισμού. Περιλαμβάνει τα μέτρα προστασίας για τη διασφάλιση της συνεχούς πρόσβασης στα δεδομένα σε περίπτωση κυβερνοεπίθεσης, ανθρώπινου λάθους, τεχνικής βλάβης ή φυσικής καταστροφής.

5.1 ΠΟΛΙΤΙΚΗ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ

Η πολιτική του Φορέα για τη λήψη αντιγράφων ασφαλείας περιλαμβάνει τα εξής:

- Καθορίζονται τα πληροφοριακά συστήματα για λήψη αντιγράφων ασφάλειας. Σε κάθε κτίριο θα πρέπει να εφαρμόζεται η τήρηση ψηφιακών αρχείων σε συστήματα δικτυακής αποθήκευσης (NAS, File Servers), από τα οποία θα λαμβάνονται αντίγραφα ασφαλείας.
- Όλα τα αντίγραφα ασφαλείας προτείνεται να είναι κρυπτογραφημένα κατά την αποθήκευση και τη μεταφορά για την προστασία της εμπιστευτικότητας των δεδομένων.
- Τύπος και συχνότητα λήψης αντιγράφων ασφαλείας: Η επιλογή του τύπου (Full, Incremental, Snapshot κ.τ.λ.) και της συχνότητας λήψης αντιγράφων ορίζεται κατά περίπτωση σύμφωνα με τις τρέχουσες συνθήκες και τις υπηρεσιακές ανάγκες του Φορέα.

5.2 ΔΟΚΙΜΕΣ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ

- Θα πραγματοποιούνται δοκιμές ανάκτησης των αντιγράφων ασφαλείας για να διασφαλιστεί η ακεραιότητα και η διαθεσιμότητα των δεδομένων.
- Όλοι οι εμπλεκόμενοι υπάλληλοι θα λαμβάνουν τακτική εκπαίδευση σχετικά με τις διαδικασίες αντιγράφων ασφαλείας και την εφαρμογή της παρούσας πολιτικής.

6. ΔΙΑΧΕΙΡΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Η Διαχείριση Περιστατικών Ασφάλειας (Incident Management) είναι η οργανωμένη διαδικασία για την ανίχνευση, αντιμετώπιση, καταγραφή και αποκατάσταση από ένα περιστατικό ασφαλείας.

Αποσκοπεί στα εξής:

- να εντοπίζονται έγκαιρα τα περιστατικά ασφαλείας,
- να καταγραφούν οι λεπτομέρειες κάθε περιστατικού ασφάλειας,
- να διερευνηθούν τα αίτια και να προσδιοριστούν οι τεχνικές ή/και οργανωτικές αδυναμίες στις οποίες ενδεχομένως οφείλεται το περιστατικό ασφάλειας,
- να καθοριστούν οι συνέπειες και να υλοποιηθούν οι ενέργειες αποκατάστασης με συγκεκριμένο χρονοδιάγραμμα, ανάλογα με την περίπτωση και
- να ενημερωθούν τα αρμόδια στελέχη του Φορέα και οι αρμόδιες Αρχές σύμφωνα με τις ισχύουσες διατάξεις.

Για τα παραπάνω θα πρέπει να υπάρχει στον Φορέα επικαιροποιημένο σχέδιο διαχείρισης περιστατικών ασφαλείας (incident response plan).

7. ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΧΕΙΑ

Ο κύριος σκοπός της Επιχειρησιακής Συνέχειας (Business Continuity - BC) είναι η διατήρηση της λειτουργικότητας της Περιφέρειας Αττικής ακόμα και υπό συνθήκες κρίσης. Αυτό επιτυγχάνεται μέσω της έγκαιρης προετοιμασίας, του σχεδιασμού και της εφαρμογής κατάλληλων διαδικασιών για την επίτευξη των παρακάτω στόχων:

- Αποτροπή διακοπής κρίσιμων λειτουργιών και ελαχιστοποίηση των επιπτώσεων.
- Ενίσχυση της ανθεκτικότητας απέναντι σε κυβερνοαπειλές και τεχνικές αποτυχίες.
- Προστασία ευαίσθητων δεδομένων και πληροφοριών από απώλεια ή παραβίαση.
- Συμμόρφωση με τις ισχύουσες νομικές και κανονιστικές διατάξεις.

Για τα παραπάνω θα πρέπει να υπάρχει στον Φορέα επικαιροποιημένο σχέδιο αποκατάστασης από καταστροφή (disaster recovery plan).

8. ΑΣΦΑΛΕΙΑ ΑΛΥΣΙΔΑΣ ΕΦΟΔΙΑΣΜΟΥ

Καθορίζονται τα μέτρα για την προστασία των πληροφοριακών υποδομών, των δεδομένων και των κρίσιμων υπηρεσιών από απειλές που σχετίζονται με προμηθευτές, υπεργολάβους και λοιπούς συνεργάτες που έχουν πρόσβαση στα συστήματα του Φορέα.

8.1 ΕΝΤΟΠΙΣΜΟΣ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΚΙΝΔΥΝΩΝ

Οι κίνδυνοι αφορούν:

- Παραβιάσεις δεδομένων, ransomware, επιθέσεις μέσω τρίτων προμηθευτών.
- Αδυναμία προμηθευτών να παραδώσουν εξαρτήματα.

8.2 ΜΕΤΡΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ

- Διατηρείται ενημερωμένο αρχείο στο οποίο καταγράφονται οι συνεργάτες-προμηθευτές οι οποίοι αποκτούν ή δύνανται να αποκτήσουν πρόσβαση στα συστήματα του Φορέα.
- Καθορισμός κριτηρίων επιλογής προμηθευτών που περιλαμβάνουν συμμόρφωση με το NIS2 και διεθνή πρότυπα κυβερνοασφάλειας.
- Καθορισμός υποχρεώσεων για προστασία δεδομένων και συνεχής παροχή υπηρεσιών.
  - ✓ Συγκεκριμένα στις συμβάσεις και στα συμφωνητικά με συνεργάτες/προμηθευτές, πρέπει να συμπεριλαμβάνονται όροι εμπιστευτικότητας και μη αποκάλυψης ευαίσθητων πληροφοριών, όροι προστασίας της ιδιωτικότητας των φυσικών προσώπων και όροι για την ασφάλεια των πληροφοριών.
- Αυστηρή διαχείριση δικαιωμάτων πρόσβασης (Least Privilege Access).
- Συλλογή πληροφοριών για κυβερνοαπειλές σε προμηθευτές. Διερεύνηση περιστατικών ασφαλείας που σχετίζονται με τρίτους και αναθεώρηση συνεργασιών όπου απαιτείται.

- Καθορισμός υποχρεώσεων για την αναφορά περιστατικών ασφαλείας εντός συγκεκριμένων χρονικών πλαισίων.
- Υποχρέωση συνεργασίας των προμηθευτών, σε διαδικασίες αντιμετώπισης και αποκατάστασης συμβάντων του Φορέα
- Διαφοροποίηση προμηθευτών για προμήθεια κρίσιμου εξοπλισμού/ εξαρτημάτων.

9. ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ

Τα μέτρα εκπαίδευσης και ευαισθητοποίησης στοχεύουν στην καλλιέργεια μιας κουλτούρας ασφάλειας στην Περιφέρεια. Περιλαμβάνουν:

- Τακτική εκπαίδευση προσωπικού σε θέματα κυβερνοασφάλειας
  - ✓ Υποχρεωτική Εκπαίδευση: Όλοι οι εργαζόμενοι υποβάλλονται σε εκπαίδευση κυβερνοασφάλειας σε τακτική βάση.
  - ✓ Εκπαίδευση ανά ρόλο: Οι εργαζόμενοι λαμβάνουν εξειδικευμένη εκπαίδευση ασφαλείας ανάλογα με τη θέση και τις αρμοδιότητές τους.
- Στοχευμένα προγράμματα πάνω σε σύγχρονους κινδύνους κυβερνοαπειλών (π.χ. phishing awareness και δοκιμαστικές επιθέσεις).
- Οδηγίες για ασφαλή χρήση υπηρεσιών και διαδικτύου.
  - ✓ Ενημερώσεις και οδηγοί για ασφαλή χρήση υπηρεσιών, διαχείριση κωδικών, αποφυγή κακόβουλου λογισμικού κ.λπ.
  - ✓ Διαρκής αξιολόγηση και αναθεώρηση: Τα προγράμματα εκπαίδευσης αναπροσαρμόζονται τακτικά ώστε να συμβαδίζουν με τις νέες απειλές και τεχνολογίες.

10. ΑΞΙΟΛΟΓΗΣΗ ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑΣ ΜΕΤΡΩΝ ΑΣΦΑΛΕΙΑΣ

Διασφαλίζεται η συνεχής βελτίωση των μέτρων ασφαλείας μέσω τακτικών αξιολογήσεων και αναθεωρήσεων. Αναλύεται σε:

- **Τακτική επαναξιολόγηση πολιτικών ασφαλείας**: Περιοδικές αναθεωρήσεις για την εξασφάλιση της συμμόρφωσης με νέες κανονιστικές απαιτήσεις και τεχνολογικές εξελίξεις.
- **Εφαρμογή δοκιμών ευπάθειας**: Τακτικοί έλεγχοι ευπάθειας και προσομοιώσεις επιθέσεων για τη βελτίωση των υφιστάμενων μηχανισμών ασφαλείας.
- **Αξιολόγηση συμβάντων ασφαλείας**: Ανάλυση όλων των περιστατικών ασφαλείας και υιοθέτηση προληπτικών μέτρων για τη μείωση κινδύνων στο μέλλον.
- **Ανατροφοδότηση από τους χρήστες**: Επικοινωνία με το προσωπικό για την καταγραφή και αναφορά θεμάτων ασφαλείας.
- **Συνεχής ενημέρωση και εκπαίδευση**: Προσαρμογή εκπαιδευτικών προγραμμάτων βάσει νέων απειλών και τάσεων στην κυβερνοασφάλεια.

11. ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

Τα μέτρα Φυσικής Ασφάλειας αφορούν τις διαδικασίες προστασίας των εγκαταστάσεων που φιλοξενούν τα κεντρικά συστήματα Πληροφορικής της Περιφέρειας Αττικής. Ο στόχος της είναι να αποτραπεί μη εξουσιοδοτημένη πρόσβαση, φυσικές καταστροφές και κακόβουλες ενέργειες, που θα μπορούσαν να θέσουν σε κίνδυνο τις πληροφορίες και τα πληροφοριακά συστήματα του Φορέα. Αναλυτικότερα εφαρμόζονται:

- Έλεγχος Πρόσβασης
- Σύστημα Συναγερμού
- Ανθεκτικότητα Υποδομών και Περιβαλλοντική Ασφάλεια
    - ✓ Χρήση UPS, γεννήτριας για προστασία από ξαφνικές διακοπές ρεύματος.
    - ✓ Συστήματα Ανίχνευσης Καπνού & Πυρκαγιάς: Σύστημα για έγκαιρη ανίχνευση και απόκριση.
    - ✓ Πυρασφάλεια: Αυτόματα συστήματα κατάσβεσης για την προστασία του εξοπλισμού.
    - ✓ Κλιματισμός: Σύστημα για διατήρηση σταθερής θερμοκρασίας και υγρασίας στα computer rooms.

12. ΕΓΚΡΙΣΗ ΚΑΙ ΙΣΧΥΣ

Η παρούσα πολιτική εγκρίνεται από τη Διοίκηση της Περιφέρειας Αττικής και τίθεται σε ισχύ από την ημερομηνία έγκρισής της. Οποιαδήποτε τροποποίηση απαιτεί έγκριση από τη Διοίκηση.

ΑΔΑ: Ψ6Λ37Λ7-ΩΞ2

@ΣΗΔΕ ΙΡΙΔΑ
682afd823e7c231e23f4decb
ΑΠ:596639
Υπογραφή: 19/05/25 13:55
Διανομή: 19/05/25 13:56

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΠΕΡΙΦΕΡΕΙΑ ΑΤΤΙΚΗΣ

ΠΟΛΙΤΙΚΗ ΟΡΘΗΣ ΧΡΗΣΗΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΑΙΟΣ 2025 - V1.0

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

Το παρόν έγγραφο αποτελεί την Πολιτική Ορθής Χρήσης Πληροφοριακών Συστημάτων της Περιφέρειας Αττικής που διαχειρίζονται και υποστηρίζονται από την Διεύθυνση Τεχνολογιών Πληροφορικής και Επικοινωνιών (Τ.Π.Ε.): αρ. 32 του Ο.Ε.Υ. (ΦΕΚ 1661/Β/2018) και καθορίζει τους κανόνες ορθής χρήσης τους, με στόχο την προστασία των δεδομένων, τη διατήρηση της ασφάλειας των συστημάτων και τη συμμόρφωση με τις ισχύουσες ρυθμίσεις και κανονισμούς.

2. ΣΚΟΠΟΣ - ΕΥΡΟΣ ΕΦΑΡΜΟΓΗΣ

Η Πολιτική Ορθής Χρήσης περιγράφει τις επιτρεπόμενες και μη επιτρεπόμενες δραστηριότητες των χρηστών των πληροφοριακών συστημάτων του Φορέα και καθορίζει την αποδεκτή χρήση του διαδικτύου, των emails και των υπηρεσιακών συσκευών από τους υπαλλήλους.
Η πολιτική αυτή έχει υποχρεωτικό χαρακτήρα και το εύρος εφαρμογής της αφορά:

- Όλους τους υπαλλήλους (μόνιμους, συμβασιούχους).
- Κάθε πρόσβαση σε δεδομένα του Φορέα, είτε εντός είτε εκτός των εγκαταστάσεων αυτού.
- Όλα τα πληροφοριακά συστήματα, τις υποδομές δικτύου, τα συστήματα ηλεκτρονικής αλληλογραφίας και τις υπηρεσιακές συσκευές.

3. ΑΠΟΔΕΚΤΗ ΧΡΗΣΗ ΕΞΟΠΛΙΣΜΟΥ /ΛΟΓΙΣΜΙΚΟΥ

Τα Πληροφοριακά Συστήματα που παραχωρούνται στους υπαλλήλους είναι περιουσιακά στοιχεία της Περιφέρειας Αττικής και ως εκ τούτου η χρήση τους πρέπει να συμμορφώνεται με την παρούσα πολιτική.

- Οι υπάλληλοι μπορούν να χρησιμοποιούν τους Η/Υ και το λογισμικό του Φορέα αποκλειστικά για υπηρεσιακούς σκοπούς.
- Επιτρέπεται η αποθήκευση και η επεξεργασία μόνο υπηρεσιακών αρχείων τόσο στους υπηρεσιακούς υπολογιστές, όσο και σε κοινόχρηστους πόρους που έχουν παρασχεθεί (π.χ. δικτυακούς δίσκους ή φακέλους). Η Διεύθυνση Τ.Π.Ε. στο

πλαίσιο άσκησης των νόμιμων καθηκόντων της και για τη διαφύλαξη σκοπών δημοσίου συμφέροντος, όπως είναι η ασφάλεια των πληροφοριακών συστημάτων, διατηρεί το δικαίωμα να ελέγξει και να διαγράψει αρχεία που θα διαπιστώσει ότι δεν είναι υπηρεσιακά, μετά από σχετική ειδοποίηση των χρηστών.

- Πρόσβαση στο διαδίκτυο επιτρέπεται μόνο για υπηρεσιακούς σκοπούς.
- Απαιτείται η χρήση ισχυρών κωδικών πρόσβασης και η τήρηση των πολιτικών ασφαλείας.
- Οι υπηρεσίες της Περιφέρειας Αττικής οφείλουν να ενημερώνουν άμεσα τη Διεύθυνση Τ.Π.Ε. μέσω του Π.Σ. ΙΡΙΔΑ, για τυχόν τροποποίηση δικαιωμάτων που έχουν εκχωρηθεί σε κάποιον υπάλληλο, (π.χ. ΙΡΙΔΑ, παροχή email, πρόσβαση σε κοινόχρηστους πόρους, απομακρυσμένη πρόσβαση κτλ.), αναφέροντας επακριβώς τα δικαιώματα που πρέπει να τροποποιηθούν/αφαιρεθούν.
- Οι υπάλληλοι οφείλουν να μη καταχρώνται πόρους του δικτύου και των συστημάτων, όπως τη διαθέσιμη χωρητικότητα συνδέσεων, τον αποθηκευτικό χώρο σκληρών δίσκων, την υπολογιστή ισχύ επεξεργαστών, την χρήση διαδικτύου για παρακολούθηση video, ακρόαση ραδιοφώνου, κ.λπ.

4. ΑΠΑΓΟΡΕΥΜΕΝΗ ΧΡΗΣΗ ΕΞΟΠΛΙΣΜΟΥ/ ΛΟΓΙΣΜΙΚΟΥ

Η χρήση των πληροφοριακών συστημάτων για μη εξουσιοδοτημένους σκοπούς απαγορεύεται αυστηρά και ειδικότερα ως απαγορευμένες ενέργειες ορίζονται οι παρακάτω:

- Χρήση των υπηρεσιακών Η/Υ για προσωπικούς σκοπούς (π.χ., social media, υπηρεσίες streaming).
- Χρήση του εξοπλισμού του Φορέα από μη εξουσιοδοτημένα πρόσωπα (επισκέπτες κ.ά.).
- Χρήση μη εγκεκριμένου λογισμικού ή εγκατάσταση εφαρμογών χωρίς την έγκριση της Διεύθυνσης Τ.Π.Ε.
- Αποθήκευση προσωπικών αρχείων και αρχείων για τα οποία μπορούν να εγείρονται θέματα πνευματικών δικαιωμάτων ή αδειοδοτήσεων (π.χ. φωτογραφίες, μουσική, βίντεο, λογισμικά κτλ.).

- Αποθήκευση ευαίσθητων δεδομένων σε μη εγκεκριμένες πλατφόρμες (Dropbox, Google Drive κ.λπ.)
- Αποστολή απόρρητων πληροφοριών εκτός του Φορέα χωρίς έγκριση.
- Κοινή χρήση κωδικών πρόσβασης ή παράκαμψη μηχανισμών ασφαλείας.
- Πρόσβαση, λήψη ή αποθήκευση ακατάλληλου ή παράνομου περιεχομένου.

5. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ ΚΑΙ ΣΥΣΚΕΥΩΝ

- Απαγορεύεται η σύνδεση στο δίκτυο του Φορέα σε συσκευές (Η/Υ, laptop, smartphone κ.ά.) που δεν ανήκουν στον Φορέα.
- Οι υπάλληλοι δεν πρέπει να χρησιμοποιούν ασύρματους προσαρμογείς (usb wifi adaptors) για ασύρματη πρόσβαση στο δίκτυο του φορέα.
- Κάθε πρίζα του δικτύου ενεργοποιείται αποκλειστικά από το αρμόδιο τμήμα της Διεύθυνσης Τ.Π.Ε. Κανένας υπάλληλος δεν έχει δικαίωμα αλλαγής της πρίζας δικτύου χωρίς την πρότερη έγκριση της αναφερθείσας Διεύθυνσης.
- Δεν επιτρέπεται η μετακίνηση Η/Υ, περιφερειακού εξοπλισμού Η/Υ (π.χ. εκτυπωτής, σαρωτής), τηλεφωνικής συσκευής, από υπάλληλο εκτός της Διεύθυνσης Τ.Π.Ε.
- Κάθε υπάλληλος φροντίζει για την ακεραιότητα του πληροφοριακού εξοπλισμού (ηλεκτρονικοί υπολογιστές, τηλέφωνα, εκτυπωτές κ.α.) του Φορέα. Σε περίπτωση που διαπιστώσει βλάβη είναι υποχρεωμένος να ενημερώνει το αρμόδιο προσωπικό της Διεύθυνσης Τ.Π.Ε.
- Προς αποφυγή μη εξουσιοδοτημένης πρόσβασης σε προσωπικά δεδομένα, με χρήση ανοιχτού υπολογιστή ο οποίος μένει χωρίς επίβλεψη (αδρανοποιημένος υπολογιστής), οι υπάλληλοι πρέπει να φροντίζουν για τα παρακάτω:
    - ✓ Ρύθμιση της αυτόματης προφύλαξης οθόνης (screen-saver) του υπολογιστή μετά από χρονικό διάστημα αδράνειας που προσδιορίζεται στα 5’, για την επανενεργοποίηση της οποίας θα απαιτείται χρήση συνθηματικού.
    - ✓ Κλείδωμα του υπολογιστή όταν απουσιάζουν πρόσκαιρα από το γραφείο τους, πιέζοντας ταυτόχρονα τα πλήκτρα ctrl + alt + delete και επιλέγοντας «Κλείδωμα».

6. ΧΡΗΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

- Επιτρέπεται η χρήση email (της μορφής xxxxxxx@patt.gov.gr) που έχει παρασχεθεί από την Περιφέρεια Αττικής ως μέσο επικοινωνίας μόνο για υπηρεσιακούς λόγους και η οποιαδήποτε ανταλλαγή μηνυμάτων θα πρέπει να έχει αυστηρά και μόνο υπηρεσιακό περιεχόμενο.
- Δεν επιτρέπεται η χρήση προσωπικών emails (Gmail, Yahoo, κ.λπ.) για υπηρεσιακά θέματα.
- Όταν ένα μήνυμα ηλεκτρονικού ταχυδρομείου έχει πολλούς αποδέκτες ή αποστέλλεται σε λίστα αποδεκτών, πρέπει να χρησιμοποιείται η κρυφή/ιδιαίτερη κοινοποίηση.
- Η διακίνηση εμπιστευτικών/απόρρητων πληροφοριών και προσωπικών δεδομένων πολιτών ή υπαλλήλων μέσω ηλεκτρονικού ταχυδρομείου, πρέπει να γίνεται με ασφαλή μετάδοση (π.χ. κρυπτογράφηση) σε συνεννόηση με τον υπηρεσιακό αποδέκτη και τη συνδρομή της Διεύθυνσης Τ.Π.Ε. Σχετικές οδηγίες υπάρχουν στο Π.Σ. ΙΡΙΔΑ και μπορεί να αναζητηθούν μέσω του όρου «κλείδωμα».
- Οι υπάλληλοι πρέπει να είναι ιδιαίτερα προσεκτικοί για περιστατικά επιθέσεων ηλεκτρονικού ψαρέματος (Phishing Attacks) και να διαχειρίζονται τα ύποπτα emails εφαρμόζοντας βασικές πρακτικές όπως:
    - ✓ <u>Έλεγχος διεύθυνσης αποστολέα (From address)</u> - Προσοχή σε ψεύτικες ή "περίεργες" διευθύνσεις. Εάν υπάρχει ασυμφωνία της διεύθυνσης email με την ιδιότητα του αποστολέα που αναφέρεται στο θέμα ή στο περιεχόμενο του email ή αν η διεύθυνση email δεν σχετίζεται λογικά με τον φερόμενο αποστολέα, το email θα πρέπει να θεωρείται δυνητικά κακόβουλο (spam/phishing).
    - ✓ <u>Έλεγχος στην ορθογραφία και τη γραμματική</u> - Πολλά spam/phishing emails έχουν συντακτικά ή ορθογραφικά λάθη, περίεργες φράσεις ή κακή μετάφραση.
    - ✓ <u>Έλεγχος των συνδέσμων (links) που υπάρχουν στο email</u> – Παρατηρούμε προσεκτικά την διεύθυνση στην οποία μας παραπέμπει ένας σύνδεσμος – link αφήνοντας για λίγα δευτερόλεπτα τον δείκτη του ποντικιού επάνω

του (εμφανίζεται κάτω αριστερά στο Outlook ή στο webmail). Αν φαίνεται περίεργο URL ή δεν ταιριάζει με τον αποστολέα, είναι ύποπτο.

- ✓ Έλεγχος στα συνημμένα αρχεία (attachments) – Προσοχή σε συνημμένα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς. Αν δεν περιμένουμε κάποιο αρχείο, ακολουθούμε τις παραπάνω οδηγίες και ελέγχους, ακόμα και αν το μήνυμα φαίνεται να προέρχεται από γνωστό αποστολέα. Σε περίπτωση αμφιβολίας για το περιεχόμενο του ηλεκτρονικού μηνύματος να ζητείται επιβεβαίωση από τον αποστολέα (π.χ. τηλεφωνική επικοινωνία μαζί του). Επιπρόσθετα, αρχεία .exe, .zip, .js, .scr, ή ακόμα και .docx / .xls δεν πρέπει να ανοίγονται με ενεργοποιημένες μακροεντολές.

7. ΔΙΑΧΕΙΡΙΣΗ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

Όλοι οι υπάλληλοι του Φορέα έχουν δικαιώματα απλού χρήστη. Σε περίπτωση που παρουσιαστεί ανάγκη εκτέλεσης ενεργειών που απαιτούν επαυξημένα δικαιώματα, θα πρέπει να επικοινωνούν με τη Διεύθυνση Τ.Π.Ε.

Οι χρήστες είναι αποκλειστικά υπεύθυνοι να συμμορφώνονται με τους κανόνες δημιουργίας ισχυρών κωδικών πρόσβασης (passwords) που είναι οι εξής:

- Να έχουν μήκος τουλάχιστον 12 χαρακτήρων.
- Να περιέχουν σωρευτικά τουλάχιστον ένα (1) κεφαλαίο γράμμα, ένα (1) μικρό γράμμα, έναν (1) αριθμό και έναν (1) ειδικό χαρακτήρα.
- Να μην περιέχουν ονόματα ή κοινές λέξεις που υπάρχουν σε λεξικά.
- Οι κωδικοί πρόσβασης πρέπει να αλλάζουν κάθε έξι (6) μήνες.
- Οι χρήστες υποχρεωτικά πρέπει να αλλάζουν οι ίδιοι το (προκαθορισμένο) συνθηματικό που τους ανατίθεται από τους διαχειριστές των συστημάτων εξαρχής.

Απαγορεύεται:

- Να γνωστοποιούνται σε άλλους χρήστες τα διαπιστευτήρια πρόσβασης.
- Να επαναχρησιμοποιούνται οι κωδικοί πρόσβασης.
- Να καταγράφονται τα διαπιστευτήρια πρόσβασης σε έντυπα μέσα, τα οποία δεν φυλάσσονται σε ασφαλές μέρος.

- Να αποθηκεύονται τα διαπιστευτήρια πρόσβασης σε ηλεκτρονική μορφή χωρίς να κρυπτογραφούνται.

8. ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΚΑΙ ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

- Οι υπάλληλοι υποχρεούνται να διασφαλίζουν την εμπιστευτικότητα των πληροφοριών και να αποκαλύπτουν δεδομένα μόνο σε εξουσιοδοτημένα τρίτα μέρη που σχετίζονται με την Υπηρεσία τους ή σε αρμόδιους συναδέλφους, σύμφωνα με τις αναθέσεις καθηκόντων που ορίζει η Διοίκηση.
- Οι υπάλληλοι είναι υπεύθυνοι για τη διατήρηση της τάξης και της οργάνωσης των ηλεκτρονικών αρχείων, διασφαλίζοντας ότι το υπηρεσιακό υλικό αποθηκεύεται σε οργανωμένους φακέλους και είναι εύκολα προσβάσιμο όταν απαιτείται.
- Σε περίπτωση που κάποιος υπάλληλος αποκτήσει πρόσβαση σε πληροφοριακό σύστημα που περιέχει δεδομένα τρίτου προσώπου (π.χ. χρήση υπολογιστή αποχωρούντος υπαλλήλου με προσωπικά ή υπηρεσιακά αρχεία), οφείλει να ενημερώσει τον αρμόδιο προϊστάμενό του.
- Η Διεύθυνση Τ.Π.Ε. έχει διαθέσει οδηγίες για την ασφαλή προστασία εγγράφων, συμπιεσμένων αρχείων και αφαιρούμενων συσκευών αποθήκευσης (π.χ. USB drives) στην βιβλιοθήκη του Π.Σ. ΙΡΙΔΑ. Οι υπάλληλοι μπορούν να αναζητήσουν αυτές τις οδηγίες μέσω του όρου «κλείδωμα». Οι οδηγίες θα επικαιροποιούνται ανάλογα με τις νέες απαιτήσεις ασφαλείας.

9. ΕΡΓΑΣΙΑ ΑΠΟ ΑΠΟΣΤΑΣΗ (REMOTE WORK POLICY)

Οι υπάλληλοι που κάνουν χρήση της υπηρεσίας απομακρυσμένης πρόσβασης στους Η/Υ της Περιφέρειας Αττικής πρέπει να συνδέονται μέσω VPN.

- Κατά τη σύνδεση μέσω VPN γίνεται χρήση 2FA (Two Factor Authentication).
- Αποστέλλονται αναλυτικές οδηγίες στους υπαλλήλους για την ασφαλή διαμόρφωση του οικιακού υπολογιστικού και δικτυακού εξοπλισμού τους.

10. ΣΥΜΜΟΡΦΩΣΗ ΚΑΙ ΥΠΟΧΡΕΩΣΕΙΣ ΧΡΗΣΤΩΝ

- Σύμφωνα με την ισχύουσα νομοθεσία, κάθε ενέργεια που μπορεί να οδηγήσει σε ζημία, ακατάλληλη χρήση, παραμέληση ή παράνομη αξιοποίηση των πληροφοριακών συστημάτων ενός δημόσιου φορέα ενδέχεται να επιφέρει πειθαρχικές και πιθανές νομικές συνέπειες.
- Όλοι οι χρήστες των πληροφοριακών πόρων της Περιφέρειας Αττικής καλούνται να υποστηρίξουν ενεργά την εφαρμογή της παρούσας πολιτικής, σύμφωνα με τον ρόλο και τις ευθύνες που τους έχουν ανατεθεί, προάγοντας πνεύμα συνεργασίας και συναδελφικότητας.
- Σε περίπτωση που οποιοσδήποτε χρήστης εντοπίσει κενό ή παράλειψη στην πολιτική αυτή, ή έχει προτάσεις βελτίωσης, μπορεί να απευθυνθεί στη Διεύθυνση Τ.Π.Ε. της Περιφέρειας Αττικής.

11. ΠΑΡΑΚΟΛΟΥΘΗΣΗ & ΕΛΕΓΧΟΣ

- Τα δεδομένα που αποθηκεύονται στους Η/Υ και στους κοινόχρηστους πόρους της Περιφέρειας Αττικής ανήκουν στον Φορέα.
- Η Διεύθυνση Τ.Π.Ε. διατηρεί το δικαίωμα να συλλέγει δεδομένα κίνησης στο δίκτυο (διεύθυνση ip, mac address, κ.ά.) τα οποία είναι προσβάσιμα μόνο από εξουσιοδοτημένο προσωπικό της Διεύθυνσης Τ.Π.Ε., δεν διατίθενται σε κανέναν τρίτο και χρησιμοποιούνται μόνο για την διενέργεια ελέγχων ασφαλείας και καλής λειτουργίας του δικτύου.

12. ΑΠΟΔΟΧΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

Όλοι οι υπάλληλοι υποχρεούνται να διαβάσουν, να κατανοήσουν και να υπογράψουν την πολιτική πριν αποκτήσουν πρόσβαση στα συστήματα του Φορέα.