Ministry of Digital Governance
Digitally signed by Ministry of Digital Governance
Date: 2026.01.30 12:30:47 EET
Reason:
Location: Athens

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΕΡΙΦΕΡΕΙΑ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΠΕΡΙΦΕΡΕΙΑΚΗ ΕΠΙΤΡΟΠΗ

Πρακτικό 4ο/27-01-2026
Απόφαση 89/2026

ΘΕΜΑ 29ο: «Έγκριση Σχεδίου Ολοκληρωμένου Προγράμματος Διαχείρισης Κινδύνων Κυβερνοασφάλειας Π.Κ.Μ. (εξ αναβολής)»

Στη Θεσσαλονίκη σήμερα, στις **27 Ιανουαρίου 2026,** ημέρα **Τρίτη** και ώρα **14:00'** μ.μ., η Περιφερειακή Επιτροπή της Π.Κ.Μ. συνήλθε σε **τακτική «με τηλεδιάσκεψη»** συνεδρίαση, κατόπιν της αριθμ. πρωτ.**Οικ. ΠΕ 50818/116/22-1-2026 (ορθή επανάληψη) προσκλήσεως της Προέδρου** αυτής, σύμφωνα με τις διατάξεις των άρθρων 175, 175Α, 176 και 177 του Ν. 3852/2010, όπως τροποποιήθηκε και ισχύει.

Στη συνεδρίαση παραβρέθηκαν:

1. Αθανασιάδου–Αηδονά Ε. Αθηνά, Περιφερειάρχης, Πρόεδρος της Π.Ε.
2. Παπουλίδης Σταμάτης, Περιφερειακός Σύμβουλος Π.Κ.Μ., Αντιπρόεδρος Π.Ε.
3. Κυριακίδου Τσιαλούκη Σιμέλα, Περιφερειακή Σύμβουλος Π.Κ.Μ., τακτικό μέλος Π.Ε.
4. Κουρτίδου Παρασκευή, Περιφερειακή Σύμβουλος, τακτικό μέλος Π.Ε.
5. Κυρίζογλου Ελευθέριος, Περιφερειακός Σύμβουλος Π.Κ.Μ., τακτικό μέλος Π.Ε.
6. Λιακόπουλος Αθανάσιος, Περιφερειακός Σύμβουλος Π.Κ.Μ., τακτικό μέλος Π.Ε.
7. Μουρτζίλας Στέργιος, Περιφερειακός Σύμβουλος Π.Κ.Μ., τακτικό μέλος Π.Ε.
8. Σωτηριάδου Αναστασία, Περιφερειακή Σύμβουλος Π.Κ.Μ., τακτικό μέλος Π.Ε.
9. Παπαστεργίου Χρήστος, Περιφερειακός Σύμβουλος Π.Κ.Μ., τακτικό μέλος Π.Ε.
10. Χαβατζάς Γεώργιος, Περιφερειακός Σύμβουλος Π.Κ.Μ., τακτικό μέλος Π.Ε.
11. Μυλόπουλος Ιωάννης, Περιφερειακός Σύμβουλος Π.Κ.Μ., τακτικό μέλος Π.Ε

Για την τήρηση των Πρακτικών συμμετείχαν οι υπάλληλοι της Π.Κ.Μ. Καμπανού Αικατερίνη, Γραμματέας της Π.Ε., Παπαγιάννη Ελισσάβετ και Οικονομίδου Αθηνά, Αναπληρώτριες Γραμματείς της Π.Ε.

Μετά τη διαπίστωση απαρτίας η Πρόεδρος της Περιφερειακής Επιτροπής κήρυξε την έναρξη της συνεδρίασης, κατά την οποία συζητήθηκαν: Θέμα 29ο της Ημερήσιας Διάταξης: «Έγκριση Σχεδίου Ολοκληρωμένου Προγράμματος Διαχείρισης Κινδύνων Κυβερνοασφάλειας Π.Κ.Μ. (εξ αναβολής)», σύμφωνα με την αριθμ. πρωτ. 893498/3266/27-11-2025 εισήγηση της Δ/νσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ., σχετικά με το ανωτέρω θέμα.

Η Περιφερειακή Επιτροπή έχοντας υπόψη:

1. Τον Ν.3852/2010 (Φ.Ε.Κ. 87/Α΄/2010) «Νέα Αρχιτεκτονική της Αυτοδιοίκησης και της Αποκεντρωμένης Διοίκησης….» όπως έχει τροποποιηθεί και ισχύει
2. Τις διατάξεις του Π.Δ.133/2010 (Φ.Ε.Κ 226/τ.Α΄/27-12-2010) «Οργανισμός της Περιφέρειας Κεντρικής Μακεδονίας» όπως τροποποιήθηκε και ισχύει με τις αριθ. 81320+77909 αποφάσεις του Γ.Γ της Α.Δ.Μ.Θ (ΦΕΚ 4302/30-12-2016)
3. Τα άρθρα 175,175Α, 176 και 177 του Ν. 3852/2010 ''περί αρμοδιοτήτων και λειτουργίας της Περιφερειακής Επιτροπής'', όπως τροποποιήθηκαν και ισχύουν σήμερα
4. Την αριθμ.15485/2023 απόφαση του Πολυμελούς Πρωτοδικείου Θεσσαλονίκης, με την οποία επικυρώθηκαν τα αποτελέσματα των εκλογών που διενεργήθηκαν στις 8 Οκτωβρίου 2023 για την ανάδειξη της Περιφερειακής Αρχής στην Περιφέρεια Κεντρικής Μακεδονίας για την περίοδο 01.01.2024 έως 31.12.2028

26ης Οκτωβρίου 64 – 54627 Θεσσαλονίκη, Τηλ. 2313 319428, 318, 315, 316, 312, 313, 314, 317,319
e-mail: pe@pkm.gov.gr

5. Την αριθ. 2/5-1-2024 (ΑΔΑ:6Ω2Ε7ΛΛ-ΙΓ3) Απόφαση του Περιφερειακού Συμβουλίου της Π.Κ.Μ. περί ‘’Εκλογής τακτικών και αναπληρωματικών μελών της Περιφερειακής Επιτροπής της Περιφέρειας Κεντρικής Μακεδονίας, για την περίοδο έως 30-6-2026, η οποία επικυρώθηκε με την αριθ. 6407/12-1-2024 Απόφαση του Γραμματέα της Αποκεντρωμένης Διοίκησης Μακεδονίας – Θράκης

6. Την αριθμ. 9/23-1-2024 απόφαση περί Εκλογής Αντιπροέδρου Περιφερειακής Επιτροπής ΠΚΜ σύμφωνα με το άρθρο 175 § 6 (ΑΔΑ: 6ΣΝΧ7ΛΛ-6ΚΛ)

7. Την αριθ. 120129/02-12-2024 διαπιστωτική πράξη περί παραίτησης του Περιφερειάρχη Κ.Μ.

8. Το Απόσπασμα πρακτικού ειδικής συνεδρίασης της αριθ.1/14-12-2024 ειδικής συνεδρίασης του επιτυχόντος συνδυασμού, «ΑΠΟΣΤΟΛΟΣ ΤΖΙΤΖΙΚΩΣΤΑΣ ΑΛΛΗΛΕΓΓΥΗ ΔΥΝΑΜΩΝΟΥΜΕ ΤΗ ΜΑΚΕΔΟΝΙΑ», για την εκλογή νέου Περιφερειάρχη Κ.Μ.

9. Την με αριθ. 125098/16-12-2024 επικύρωση εκλογής νέου Περιφερειάρχη της Π.Κ.Μ. από τον Γραμματέα Αποκεντρωμένης Διοίκησης Μακεδονίας – Θράκης

10. Την αριθμ. Γ.Π.Κ.Μ./οικ.252/22-1-2024 απόφαση του Περιφερειάρχη Π.Κ.Μ. «περί ορισμού Γραμματέως της Περιφερειακής Επιτροπής της Π.Κ.Μ.» (ΑΔΑ:Ψ0997ΛΛ-ΧΚΣ)

11. Τον 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" (Φ.Ε.Κ. Α' 195/2024)

12. Την Κοινή Υπουργική Απόφαση 1689/30-4-25 "Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων" (ΦΕΚ Β' 2186/2025)

13. Την αριθμ. 1949/2025 απόφαση της Περιφερειακής Επιτροπής Περιφέρειας Κεντρικής Μακεδονίας, με την οποία αναβλήθηκε η συζήτηση του θέματος «Έγκριση ολοκληρωμένου Προγράμματος Διαχείρισης Κινδύνων Κυβερνοασφάλειας Π.Κ.Μ.»

14. Το αριθμ. πρωτ. 50907(250)/22-01-2026 έγγραφο της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης ΠΚΜ περί μη δημοσίευσης σε ΦΕΚ του Σχεδίου Ασφάλειας Πληροφοριακών Συστημάτων της ΠΚΜ

15. Την υπ’ αριθμ. πρωτ οικ. 977192(3585)/29-12-2025 εισήγηση της Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ., η οποία έχει ως εξής:

ΘΕΜΑ: Έγκριση Ολοκληρωμένου Προγράμματος Διαχείρισης Κινδύνων Κυβερνοασφάλειας Π.Κ.Μ.

Σχετ:

1. *Ο Ν. 3852/2010 «Νέα Αρχιτεκτονική της Αυτοδιοίκησης και της Αποκεντρωμένης Διοίκησης – Πρόγραμμα Καλλικράτης» (ΦΕΚ Α΄ 87/ 2010), όπως ισχύει.*
2. *Οι υπ' αριθμ. 81320 και 77909/01-12-2016 αποφάσεις του Γενικού Γραμματέα της Αποκεντρωμένης Διοίκησης Μακεδονίας - Θράκης (ΦΕΚ. 4302./τ. Α΄/ 30-12-2016), με τις οποίες εγκρίθηκε η τροποποίηση του Οργανισμού της Π.Κ.Μ. (Π.Δ 133/2010, ΦΕΚ Α΄ 226/ 2010).*
3. *Το άρθρο 7 της υπ’ αριθμ. 17255(397)/09.01.2024 απόφασης Περιφερειάρχη Κεντρικής Μακεδονίας, περί μεταβίβασης αρμοδιοτήτων και παροχής εξουσιοδότησης υπογραφής εγγράφων, αποφάσεων και άλλων πράξεων «ΜΕ ΕΝΤΟΛΗ ΠΕΡΙΦΕΡΕΙΑΡΧΗ» (ΑΔΑ: ΨΛΤΑ7ΛΛ-Σ93, ΦΕΚ Β΄148/2024).*
4. *Ο 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" (Φ.Ε.Κ. Α' 195/2024).*
5. *Η Κοινή Υπουργική Απόφαση 1689/30-4-25 "Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων" (Φ.Ε.Κ. Β' 2186/2025).*

Ως βασική οντότητα στον τομέα της κυβερνοασφάλειας κατά την έννοια του άρθρου 4 του Ν. 5160/2024, η Π.Κ.Μ. υποχρεούται κατόπιν του άρθρου 4 της Κ.Υ.Α. 1689/2025 για τη διαμόρφωση και εφαρμογή Ολοκληρωμένου Προγράμματος Διαχείρισης Κινδύνων Κυβερνοασφάλειας.

26ης Οκτωβρίου 64 – 54627 Θεσσαλονίκη, Τηλ. 2313 319428, 318, 315, 316, 312, 313, 314, 317,319
e-mail: pe@pkm.gov.gr

Το Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας Π.Κ.Μ. σε συμμόρφωση με το άρθρο 4α της Κ.Υ.Α. 1689/2025, αποτελείται από πολιτικές ασφάλειας εντός των οποίων ορίζονται οι σχετικές πληροφορίες περί διαδικασιών, ανάθεσης ρόλων, αρμοδιοτήτων και ευθυνών, καθώς και τεχνικών, οργανωτικών και επιχειρησιακών μέτρων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών της Π.Κ.Μ. Οι πολιτικές ασφάλειας που εφαρμόζονται προκύπτουν από το άρθρο 6β της Κ.Υ.Α. 1689/2025 και παράλληλα εντός αυτών, συμπεριλαμβάνεται το σύνολο των μέτρων και διαδικασιών που ορίζονται στα υπόλοιπα άρθρα της εν λόγω Κ.Υ.Α.

Λαμβάνοντας υπόψη τα ανωτέρω καθώς και τα οριζόμενα στην παρ. 1 περ. ιζ του άρθρου 176 του Ν. 3852/10, όπως ισχύουν, επισυνάπτουμε το σχέδιο του Ολοκληρωμένου Προγράμματος Διαχείρισης Κινδύνων Κυβερνοασφάλειας Π.Κ.Μ. και παρακαλούμε την Περιφερειακή Επιτροπή Κ.Μ. όπως προβεί σε εισήγηση προς το Περιφερειακό Συμβούλιο Κ.Μ. για την έκδοση απόφασης Περιφερειακού Συμβούλιου Κ.Μ. περί «Έγκρισης Ολοκληρωμένου Προγράμματος Διαχείρισης Κινδύνων Κυβερνοασφάλειας Π.Κ.Μ.».

Παραμένουμε στη διάθεση σας για οποιαδήποτε λοιπή πληροφορία.

***Συν.:** Σχέδιο Ο.Π.Δ.Κ.Κ. Π.Κ.Μ.*

Μ.Ε.Π.
Ο ΑΝΤΙΠΕΡΙΦΕΡΕΙΑΡΧΗΣ
ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Ν. ΤΖΟΛΛΑΣ

Τη διαλογική συζήτηση και την ψηφοφορία που ακολούθησε, κατά την οποία οι κ.κ. Παπαστεργίου Χ. και Παπουλίδης Στ. έδωσαν λευκή ψήφο, ο κ. Χαβατζάς Γ. έδωσε αρνητική ψήφο, ο κ. Μυλόπουλος Ι. δήλωσε παρών, ενώ όλα τα υπόλοιπα μέλη της Επιτροπής έδωσαν θετική ψήφο και ως εκ τούτου η Περιφερειακή Επιτροπή

α π ο φ α σ ί ζ ε ι κατά πλειοψηφία
(μειοψηφούντος του κ. Χαβατζά Γ.)

Να εισηγηθεί στο Περιφερειακό Συμβούλιο Κ.Μ. την έγκριση του συνημμένου Σχέδιου Ολοκληρωμένου Προγράμματος Διαχείρισης Κινδύνων Κυβερνοασφάλειας Π.Κ.Μ., που αποτελεί αναπόσπαστο τμήμα της παρούσης.

Σημειώνεται ότι, σύμφωνα με τον ν. 5160/2024, την ΚΥΑ 1689/2025 και το αριθμ. πρωτ. 50907/250)/22-01-2026 έγγραφο της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης ΠΚΜ, δεν απαιτείται δημοσίευση στο Φύλλο Εφημερίδας της Κυβέρνησης.

Η απόφαση αυτή πήρε α/α 89/2026

Η Περιφερειάρχης & Πρόεδρος
της Περιφερειακής Επιτροπής
Περιφέρειας Κεντρικής Μακεδονίας

Αθανασιάδου - Αηδονά Ε. Αθηνά

Τα μέλη

Η Γραμματέας

Αικατερίνη Καμπανού

ΠΕΡΙΦΕΡΕΙΑΚΗ ΕΠΙΤΡΟΠΗ ΠΕΡΙΦΕΡΕΙΑΣ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ Απόφαση 89/27-01-2026
26ης Οκτωβρίου 64 – 54627 Θεσσαλονίκη, Τηλ. 2313 319428, 318, 315, 316, 312, 313, 314, 317,319
e-mail: pe@pkm.gov.gr

ΠΕΡΙΦΕΡΕΙΑ
ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΑΝΤΙΠΕΡΙΦΕΡΕΙΑ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας

Περιεχόμενα

Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κίνδυνων Κυβερνοασφάλειας Π.Κ.Μ.

Εισαγωγή

Αναγνωρίζοντας τον ρόλο της ως η μεγαλύτερη σε έκταση και η δεύτερη σε πληθυσμό Περιφέρεια της χώρας, η Π.Κ.Μ. αντιμετωπίζει με αυξημένη υπευθυνότητα την προστασία των ψηφιακών υποδομών της, διασφαλίζοντας την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών που διαχειρίζεται, στο πλαίσιο της εύρυθμης λειτουργίας των ψηφιακών υπηρεσιών και της εμπιστοσύνης των πολιτών.

Ως βασική οντότητα κατά την έννοια του άρθρου 4 του Ν. 5160/2024, η Π.Κ.Μ. διαμορφώνει και εφαρμόζει Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας, σύμφωνα με το άρθρο 4 της Κ.Υ.Α. 1689/2025.

Σκοπός του παρόντος προγράμματος είναι η εξασφάλιση:

- Της προστασίας των πληροφοριακών και ψηφιακών αγαθών της Π.Κ.Μ.
- Της ανθεκτικότητας των ψηφιακών υπηρεσιών κρίσιμης σημασίας.
- Της προληπτικής διαχείρισης κινδύνων κυβερνοασφάλειας.
- Της διαρκούς συμμόρφωσης της Π.Κ.Μ. με την ισχύουσα Νομοθεσία περί κυβερνοασφάλειας.

Νομικό και Ρυθμιστικό Πλαίσιο

Το Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας Π.Κ.Μ. συμμορφώνεται με:

- Τον Νόμο 5160/2025 *«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».*
- Την Κοινή Υπουργική Απόφαση 1689/2025 *«Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων».*

Δομή του Προγράμματος

Το Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας Π.Κ.Μ. σε συμμόρφωση με το άρθρο 4α της Κ.Υ.Α. 1689/2025, αποτελείται από πολιτικές ασφάλειας εντός των οποίων ορίζονται οι σχετικές πληροφορίες περί διαδικασιών, ανάθεσης ρόλων, αρμοδιοτήτων και ευθυνών, καθώς και τεχνικών, οργανωτικών και επιχειρησιακών μέτρων για την ασφάλεια των συστημάτων δικτύου και πληροφοριών της Π.Κ.Μ.

Οι πολιτικές ασφάλειας που εφαρμόζονται προκύπτουν από το άρθρο 6β της Κ.Υ.Α. 1689/2025. Παράλληλα, εντός των πολιτικών ασφάλειας συμπεριλαμβάνεται το σύνολο των μέτρων και διαδικασιών που ορίζονται στα υπόλοιπα άρθρα της εν λόγω Κ.Υ.Α.

1. Γενική Πολιτική Ασφάλειας Πληροφοριών

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

1.1 Σκοπός

Η παρούσα πολιτική συντάχθηκε σύμφωνα με την ΚΥΑ 1689/2025 και καθορίζει τις βασικές αρχές, τους κανόνες και τους ρόλους που διέπουν την ασφάλεια πληροφοριών και συστημάτων της Περιφέρειας Κεντρικής Μακεδονίας.

Στόχος της είναι να εδραιώσει ένα ενιαίο θεσμικό πλαίσιο για την προστασία των ψηφιακών αγαθών, των δεδομένων και των κρίσιμων υπηρεσιών, και να εξασφαλίσει την ορθή και αποτελεσματική εφαρμογή των θεματικών πολιτικών και διαδικασιών κυβερνοασφάλειας.

1.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε όλα τα συστήματα πληροφορικής, δίκτυα, υποδομές, δεδομένα, εφαρμογές, και υπηρεσίες που λειτουργούν ή εποπτεύονται από την Π.Κ.Μ καθώς και στις διαδικασίες που αφορούν το ανθρώπινο δυναμικό της ΠΚΜ και τις σχέσεις με την εφοδιαστική αλυσίδα.

1.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής και των θεματικών πολιτικών ασφάλειας (ΚΥΑ 1689/2025, αρθ.4).
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την εξασφάλιση της ασφάλειας και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά (αρ. 17255(397)/09-01-24 απόφαση Περιφερειάρχη Π.Κ.Μ., άρθρο 7).
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής και των θεματικών πολιτικών ασφάλειας καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική και στις θεματικές πολιτικές ασφάλειας.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική και στις θεματικές πολιτικές ασφάλειας.

- **Προϊστάμενοι Οργανικών Μονάδων Π.Κ.Μ.:** Υπεύθυνοι για την ενημέρωση των υφισταμένων τους περί της αναγκαιότητας συμμόρφωσης τους με τα οριζόμενα στην παρούσα πολιτική και στις θεματικές πολιτικές ασφάλειας της Π.Κ.Μ. με ιδιαίτερη έμφαση στην Πολιτική Ορθής Χρήσης Αγαθών και Δεδομένων.
- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική και στις θεματικές πολιτικές ασφάλειας της Π.Κ.Μ.

1.4 Βασικές Αρχές Ασφάλειας Πληροφοριών και Κυβερνοασφάλειας

Οι παρακάτω αρχές καθορίζουν το θεμελιώδες πλαίσιο πάνω στο οποίο βασίζεται η διαχείριση των κίνδυνων που προκύπτουν κατά τη χρήση Τεχνολογιών Πληροφορικής και Επικοινωνιών (Τ.Π.Ε.) από την Π.Κ.Μ.

1.4.1 Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα:

Η προστασία των πληροφοριακών αγαθών της Π.Κ.Μ. στηρίζεται στην τήρηση των τριών θεμελιωδών αρχών ασφάλειας: Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα.

1.4.2 Λογοδοσία και Ιχνηλασιμότητα Ενεργειών:

Όλες οι κρίσιμες ενέργειες σε συστήματα και δεδομένα πρέπει να είναι ανιχνεύσιμες μέσω κατάλληλων μηχανισμών καταγραφής, ώστε να διασφαλίζεται η λογοδοσία.

1.4.3 Ελαχιστοποίηση Δικαιωμάτων Πρόσβασης

Η πρόσβαση σε πληροφορίες, πόρους και συστήματα περιορίζεται στο ελάχιστο απαραίτητο για την εκτέλεση των καθηκόντων του χρήστη (least privilege). Η απόδοση δικαιωμάτων πραγματοποιείται βάσει ρόλων (Role-Based Access Control - RBAC) και τεκμηριώνεται.

1.4.4 Εκτίμηση και Διαχείριση Κινδύνων

Η Π.Κ.Μ. εφαρμόζει δομημένο και τεκμηριωμένο πλαίσιο διαχείρισης κινδύνων κυβερνοασφάλειας το οποίο περιλαμβάνει διαδικασία εκτίμησης κινδύνων (risk assessment) και τεχνικά και οργανωτικά μέτρα για την αντιμετώπισή τους (risk treatment).

1.4.5 Ασφάλεια Εφοδιαστικής Αλυσίδας και τρίτων μερών

Οι προμηθευτές, πάροχοι υπηρεσιών και τα λοιπά τρίτα μέρη αξιολογούνται και εντάσσονται στο πλαίσιο ασφάλειας της Π.Κ.Μ. μέσω συμβατικών υποχρεώσεων και ελέγχου συμμόρφωσης.

1.4.6 Ενημέρωση, Ευαισθητοποίηση και Ασφάλεια Ανθρώπινου Δυναμικού

Το προσωπικό της Π.Κ.Μ. ενημερώνεται για τις υποχρεώσεις του ως προς την κυβερνοασφάλεια.

Πραγματοποιούνται ετήσιες δράσεις ευαισθητοποίησης για μη τεχνικό προσωπικό με εστίαση σε phishing και social engineering.

1.5 Νομική και Κανονιστική Συμμόρφωση

Η Π.Κ.Μ. τηρεί τα απαραίτητα μέτρα και διαδικασίες ώστε να συμμορφώνεται με:

- Τον Νόμο 5160/2025 *«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»*.
- Την Κοινή Υπουργική Απόφαση 1689/2025 *«Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων»*.

Οι πολιτικές ασφάλειας της Π.Κ.Μ. λαμβάνουν υπόψη ότι οι απαιτήσεις της Ευρωπαϊκής Οδηγίας NIS2, όπως αυτή εφαρμόζεται στην Ελληνική Νομοθεσία με τον Ν. 5160/2024 και την Κ.Υ.Α. 1689/2025, είναι διακριτές από τις απαιτήσεις συμμόρφωσης με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ - GDPR).

Τα τεχνικά, οργανωτικά και φυσικά μέτρα ασφάλειας που περιλαμβάνονται στις πολιτικές ασφάλειας συμβάλλουν πέραν των άλλων και στην προστασία των προσωπικών δεδομένων, χωρίς να αντικαθιστούν τον ρόλο και τις αρμοδιότητες του Υπευθύνου Προστασίας Δεδομένων (DPO) της Π.Κ.Μ.

1.6 Θεματικές Πολιτικές

Η Γενική Πολιτική Ασφάλειας υποστηρίζεται από τις εξής 13 θεματικές πολιτικές ασφάλειας:

- Πολιτική Ελέγχου Πρόσβασης
- Πολιτική Διαχείρισης και Ασφαλούς Παραμετροποίησης Αγαθών
- Πολιτική Ορθής Χρήσης Αγαθών και Δεδομένων
- Πολιτική Αφαιρούμενων Μέσων Αποθήκευσης
- Πολιτική Επιχειρησιακής Συνέχειας, Διαχείρισης Περιστατικών και Κρίσεων
- Πολιτική Ασφάλειας Εφοδιαστικής Αλυσίδας
- Πολιτική Ασφάλειας Δικτύων
- Πολιτική Διαχείρισης Κινδύνων και Παρακολούθησης Συμμόρφωσης
- Πολιτική Αντιγράφων Ασφαλείας
- Πολιτική Κρυπτογράφησης Δεδομένων και Επικοινωνιών
- Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας
- Πολιτική Ασφάλειας Ανθρώπινου Δυναμικού & Εκπαίδευσης

Η Γενική Πολιτική Ασφάλειας και οι θεματικές πολιτικές εγκρίνονται από το Περιφερειακό Συμβούλιο και επικαιροποιούνται:

- Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων.
- Μετά από εμφάνιση σοβαρού περιστατικού.
- Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας.

2. Πολιτική Ελέγχου Πρόσβασης

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

2.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι η θέσπιση αρχών και κατευθύνσεων για τον έλεγχο της πρόσβασης στα πληροφοριακά συστήματα, δεδομένα και ψηφιακές υποδομές της Περιφέρειας Κεντρικής Μακεδονίας, με στόχο τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και των υπηρεσιών.

2.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική καλύπτει όλους τους μηχανισμούς, διαδικασίες και κανόνες που σχετίζονται με τη χορήγηση, διαχείριση, παρακολούθηση και ανάκληση της πρόσβασης σε πληροφοριακά συστήματα, εφαρμογές και δεδομένα της Περιφέρειας Κεντρικής Μακεδονίας, ανεξαρτήτως μέσου ή τοποθεσίας πρόσβασης.

2.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την ασφάλεια και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας

Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική.

2.4 Μέτρα Ασφάλειας

2.4.1 Κεντρική Υπηρεσία Ταυτοποίησης

Σύνδεση πληροφοριακών συστημάτων με κεντρική υπηρεσία ταυτοποίησης και εξουσιοδότησης χρηστών (λ.χ. Active Directory), όπου αυτό είναι εφικτό σε τεχνικό επίπεδο, για λόγους εξοικονόμησης πόρων (σε προγραμματισμό και διαχείριση) και γενικευμένης χρήσης ενός κεντρικού λογαριασμού χρήστη.

2.4.2 Κατάλογος Λογαριασμών

Διατήρηση επικαιροποιημένου καταλόγου με όλους τους λογαριασμούς χρηστών, ο οποίος περιέχει κατ' ελάχιστον το ονοματεπώνυμο, την ημερομηνία έναρξης / λήξης και τα δικαιώματα πρόσβασης του λογαριασμού.

2.4.3 Μοναδική Ταυτότητα Χρήστη/Συστήματος

Απόδοση μοναδικής ταυτότητας σε κάθε χρήστη και σύστημα που αποκτά πρόσβαση στα πληροφοριακά συστήματα ή δεδομένα της Π.Κ.Μ.

2.4.4 Δικαιώματα Πρόσβασης

Χορήγηση και διαχείριση δικαιωμάτων πρόσβασης σύμφωνα με τις αρχές του ελάχιστου αναγκαίου προνομίου (least privilege), της ανάγκης γνώσης (need to know) και του διαχωρισμού καθηκόντων.

2.4.5 Περιορισμός Προνομιούχων Λογαριασμών

Περιορισμός της χρήσης προνομιούχων λογαριασμών (λογαριασμοί με αυξημένα δικαιώματα) στον απολύτως απαραίτητο βαθμό.

2.4.6 Χρήση Δεύτερου Λογαριασμού

Χορήγηση δεύτερου standard λογαριασμού απλού χρήστη (non-privileged account) για την εκτέλεση μη διαχειριστικών εργασιών καθημερινής ρουτίνας, στους χρήστες που λόγω καθηκόντων διαθέτουν επίσης λογαριασμό αυξημένων προνομίων.

2.4.7 Αναθεώρηση / Ανάκληση Προσβάσεων

Έγκαιρη αναθεώρηση ή ανάκληση προσβάσεων χρηστών σε περίπτωση μεταβολής καθηκόντων ή λήξης σχέσης εργασίας με την Π.Κ.Μ.

2.4.8 Πολιτική Σύνθετων Κωδικών

Εξαναγκασμός χρήσης σύνθετων κωδικών πρόσβασης, η πολυπλοκότητα των οποίων είναι σύμφωνη με τις ισχύουσες ρυθμιστικές απαιτήσεις και τα σχετικά διεθνή πρότυπα ασφάλειας.

2.4.9 Πολυπαραγοντική Αυθεντικοποίηση (MFA)

Εφαρμογή πολυπαραγοντικής αυθεντικοποίησης σε διαχειριστικά συστήματα που είναι προσβάσιμα μέσω του διαδικτύου (λ.χ. κονσόλες διαχείρισης που φιλοξενούνται σε cloud περιβάλλοντα).

2.4.10 Κρυπτογράφηση Διαπιστευτηρίων

Αποθήκευση κωδικών πρόσβασης εντός των πληροφοριακών συστημάτων που υλοποιούν διαδικασίες αυθεντικοποίησης αποκλειστικά σε μη αναστρέψιμη,

κρυπτογραφικά ασφαλή μορφή, με τη χρήση κατάλληλων συναρτήσεων κατακερματισμού (hash functions). Δεν επιτρέπεται η αποθήκευση κωδικών σε απλό κείμενο (plaintext).

2.4.11 Αυτόματο Κλείδωμα Λογαριασμών

Αυτόματο κλείδωμα λογαριασμών έπειτα από προκαθορισμένο αριθμό αποτυχημένων προσπαθειών αυθεντικοποίησης, για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

2.4.12 Αυτόματη Προφύλαξη Οθόνης

Αυτόματη ενεργοποίηση προφύλαξης οθόνης (screen saver) ύστερα από προκαθορισμένο χρονικό διάστημα αδράνειας, σε όλους τους σταθμούς εργασίας.

2.4.13 Περιοδική Αξιολόγηση Δικαιωμάτων Πρόσβασης

Περιοδική αξιολόγηση και επικαιροποίηση εφ' όσον απαιτείται, των δικαιωμάτων πρόσβασης.

2.4.14 Περιοδική Αξιολόγηση Μέτρων Ελέγχου Πρόσβασης

Περιοδική αξιολόγηση και επικαιροποίηση εφ' όσον απαιτείται, των μέτρων και διαδικασιών ελέγχου πρόσβασης, ιδίως σε περιπτώσεις σημαντικών αλλαγών στα πληροφοριακά συστήματα της Π.Κ.Μ. ή σε περιπτώσεις εμφάνισης περιστατικών ασφάλειας.

3. Πολιτική Διαχείρισης και Ασφαλούς Παραμετροποίησης Αγαθών

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

3.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι η δημιουργία ενός πλαισίου για τη διαχείριση και την ασφαλή παραμετροποίηση του συνόλου των πληροφοριακών αγαθών της Περιφέρειας Κεντρικής Μακεδονίας, διασφαλίζοντας ότι τα πληροφοριακά αγαθά αναγνωρίζονται, καταγράφονται, ταξινομούνται, είναι διαχειριζόμενα και ασφαλώς παραμετροποιημένα καθ' όλη τη διάρκεια του κύκλου ζωής τους.

3.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε όλα τα πληροφοριακά αγαθά της ΠΚΜ: υλικό, λογισμικό, δεδομένα, είτε αυτά φιλοξενούνται στις εγκαταστάσεις της Π.Κ.Μ. (on-premise) είτε σε εγκαταστάσεις τρίτων (λ.χ. cloud τρίτων Εταιρειών ή Φορέων).

3.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την ασφάλεια και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική.

3.4 Μέτρα Ασφάλειας

Διαχείριση Αγαθών

3.4.1 Κατάλογος Αγαθών Πληροφορικής
Τήρηση ενημερωμένου καταλόγου με τα αγαθά πληροφορικής (υλικό & λογισμικό) είτε φιλοξενούνται στις εγκαταστάσεις της Π.Κ.Μ. (on-premise) ή σε εγκαταστάσεις τρίτων (λ.χ. cloud τρίτων Εταιρειών ή Φορέων).

3.4.2 Μοναδικό Αναγνωριστικό Αγαθού
Χαρακτηρισμός κάθε αγαθού από μοναδικό αναγνωριστικό κωδικό.

3.4.3 Άμεση Καταγραφή Νέων Αγαθών
Καταγραφή κάθε νέου αγαθού στον κατάλογο αγαθών άμεσα, μετά την απόκτηση ή δημιουργία του.

3.4.4 Ιδιοκτησία Αγαθού
Ορισμός ιδιοκτήτη (owner) σε κάθε αγαθό που τηρείται στον κατάλογο, με σκοπό την ενίσχυση της ευθύνης και λογοδοσίας, καθ' όλη τη διάρκεια του κύκλου ζωής του αγαθού.

3.4.5 Ταξινόμηση Αγαθών
Ταξινόμηση αγαθών σε διακριτές ομάδες (groups) ανάλογα με την κρισιμότητα και ευαισθησία τους σε σχέση με τη λειτουργία της Π.Κ.Μ.

3.4.6 Επικαιροποίηση Καταλόγου
Διενέργεια τακτικών ελέγχων για τη διασφάλιση της ακρίβειας του καταλόγου αγαθών πληροφορικής.

3.4.7 Απόσυρση Μη Υποστηριζόμενου Εξοπλισμού/Λογισμικού
Απόσυρση εξοπλισμού, λειτουργικών συστημάτων και εφαρμογών για τα οποία έχει σταματήσει η υποστήριξη από τον κατασκευαστή ή πάροχο.

3.4.8 Ασφαλής Απόσυρση Αγαθών
Μέριμνα για την ασφαλή απόσυρση των πληροφοριακών αγαθών και ιδιαιτέρως του υλικού, σύμφωνα με την κείμενη νομοθεσία και τις εσωτερικές πολιτικές ασφαλείας της Π.Κ.Μ.

Ασφαλής Παραμετροποίηση Αγαθών

3.4.9 Αλλαγή Default Passwords
Τροποποίηση προεπιλεγμένων συνθηματικών (default passwords) κατά την αρχική παραμετροποίηση κάθε νέου προϊόντος, συστήματος ή εφαρμογής.

3.4.10 Επιβολή Ρυθμίσεων και Παραμετροποιήσεων
Αυτοματοποιημένη επιβολή ρυθμίσεων και παραμετροποιήσεων στα πληροφοριακά αγαθά μέσω διαδικασιών και εργαλείων (λ.χ μέσω πολιτικών ομάδας Active Directory), όπου αυτό είναι τεχνικά εφικτό.

3.4.11 Διαδικασίες Ασφαλούς Παραμετροποίησης
Υλοποίηση διαδικασιών ασφαλούς παραμετροποίησης (secure configuration) για το σύνολο του υλικού, του λογισμικού, των υπηρεσιών και του δικτύου της Π.Κ.Μ., αξιοποιώντας μεθόδους όπως:

- Χρήση προκαθορισμένων πρότυπων κατασκευαστών ή ανεξάρτητων ερευνητικών οργανισμών.
- Εφαρμογή γενικών αρχών κυβερνοασφάλειας, όπως η αρχή της ελάχιστης λειτουργικότητας (least functionality) και η αρχή των ελάχιστων προνομίων (least privilege).

3.4.12 Χρήση Υποστηριζόμενων Εκδόσεων Λειτουργικού και Λογισμικού

Χρήση μόνο υποστηριζόμενων εκδόσεων λειτουργικών συστημάτων σε σταθμούς εργασίας, εξυπηρετητές και δικτυακές συσκευές και μέριμνα για αυτόματη λήψη και εγκατάσταση των σχετικών ενημερώσεων λειτουργικού και λογισμικού όπου αυτό είναι τεχνικά εφικτό και ασφαλές.

3.4.13 Απενεργοποίηση Περιττών Υπηρεσιών

Απενεργοποίηση κάθε περιττής υπηρεσίας (service) σε σταθμούς εργασίας και εξυπηρετητές.

Προστασία από Κακόβουλο Λογισμικό

3.4.14 Λογισμικό Προστασίας από Κακόβουλο Λογισμικό

Χρήση λογισμικού προστασίας από κακόβουλο λογισμικό σε σταθμούς εργασίας και εξυπηρετητές και διαχείριση αυτού μέσω κεντρικής κονσόλας.

3.4.15 Έλεγχος Εκτέλεσης Εφαρμογών

Χρήση τεχνολογιών για τον έλεγχο της εκτέλεσης εφαρμογών και ανίχνευσης μη εξουσιοδοτημένων τύπων λογισμικού, σε σταθμούς εργασίας και εξυπηρετητές.

3.4.16 Φιλτράρισμα email

Χρήση τεχνολογιών ανίχνευσης και φιλτραρίσματος μηνυμάτων ηλεκτρονικού ταχυδρομείου, για τον εντοπισμό και την απόρριψη κακόβουλων ή ανεπιθύμητων μηνυμάτων.

3.4.17 Χρήση Ενημερωμένων Φυλλομετρητών

Επιβολή χρήσης μόνο υποστηριζόμενων φυλλομετρητών (web browsers) σε σταθμούς εργασίας χρηστών, και μέριμνα για την τακτική ενημέρωσή τους, καθώς και για τον περιορισμό της εγκατάστασης σε αυτούς περιττών ή μη εξουσιοδοτημένων επεκτάσεων (extensions) τρίτων παρόχων.

3.4.18 Φιλτράρισμα Domain

Χρήση τεχνολογιών φιλτραρίσματος για την απαγόρευση σύνδεσης των συστημάτων δικτύου και πληροφοριών της Π.Κ.Μ. με γνωστά κακόβουλα ονόματα χώρου (domains) και ιστοτόπους.

3.4.19 Τείχος Προστασίας ως Εφαρμογή

Χρήση τείχους προστασίας ως εφαρμογή (host-based firewall) σε κάθε σταθμό εργασίας και εξυπηρετητή, το οποίο εμποδίζει κάθε δικτυακή σύνδεση προς τη συσκευή, με εξαίρεση τις ελάχιστες θύρες και υπηρεσίες που απαιτούνται βάσει των επιχειρησιακών αναγκών.

3.4.20 Host-based Intrusion Prevention Systems

Χρήση συστήματος πρόληψης εισβολών (host-based Intrusion prevention system) σε εξυπηρετητές και σταθμούς εργασίας που διαθέτουν λειτουργικό σύστημα Windows.

3.4.21 Αποτροπή Τροποποίησης Ρυθμίσεων Ασφάλειας

Διασφάλιση μη δυνατότητας τροποποίησης ρυθμίσεων ασφάλειας σταθμών εργασίας, από χρήστες στους οποίους έχουν αποδοθεί standard δικαιώματα (non-privileged users).

3.4.22 Περιοδική Επικαιροποίηση Παραμετροποιήσεων

Αξιολόγηση και επικαιροποίηση των διαδικασιών ασφαλούς παραμετροποίησης σε περιοδική βάση καθώς και όταν νέες απειλές και ευπάθειες γίνονται γνωστές ή κατόπιν εμφάνισης σοβαρού περιστατικού ασφάλειας.

Διαχείριση Αλλαγών σε Παραμετροποιήσεις

3.4.23 Διαχείριση Αλλαγών σε Παραμετροποιήσεις

Εφαρμογή διαδικασιών για τη διαχείριση των αλλαγών στα συστήματα δικτύου και πληροφοριών της Π.Κ.Μ. οι οποίες περιλαμβάνουν κατ' ελάχιστον:

- Την αξιολόγηση του πιθανού αντικτύπου των αλλαγών.
- Τον ορισμό κριτηρίων για την κατηγοριοποίηση και προτεραιοποίηση των αλλαγών.
- Την υλοποίηση των αλλαγών βάσει συγκεκριμένου πλάνου.
- Την πραγματοποίηση δοκιμών για τις αλλαγές όπου αυτό κρίνεται απαραίτητο.

Ασφαλής Ανάπτυξη Εφαρμογών

3.4.24 Ασφάλεια Εφαρμογών από το Στάδιο του Σχεδιασμού

Ορισμός απαιτήσεων ασφάλειας των εφαρμογών που η Π.Κ.Μ. αποκτά ή αναπτύσσει, ήδη από το στάδιο του σχεδιασμού και των προδιαγραφών, με βάση την κρισιμότητα των εφαρμογών και τους κινδύνους που σχετίζονται με τη λειτουργία τους.

3.4.25 Αρχές Ασφαλούς Κώδικα και Αρχιτεκτονικής

Υλοποίηση αρχών συγγραφής ασφαλούς κώδικα και ασφαλούς αρχιτεκτονικής για τις εφαρμογές που η Π.Κ.Μ. αποκτά ή αναπτύσσει, όπως λ.χ. οι αρχές της «ασφάλειας από το σχεδιασμό» (security by design), της «ασφάλειας εξ ορισμού» (security by default), των «ελάχιστων προνομίων» (least privilege), καθώς και της «μηδενικής εμπιστοσύνης» (zero-trust).

3.4.26 Διαχωρισμός Περιβαλλόντων Dev/Test/Prod

Διαχωρισμός των περιβάλλοντων ανάπτυξης, δοκιμών και παραγωγής των εφαρμογών που η Π.Κ.Μ. αποκτά ή αναπτύσσει και προστασία αυτών με κατάλληλα μέτρα ασφάλειας όπως λ.χ., διαχωρισμός δικτύων, ασφαλής διαμόρφωση συστημάτων, έλεγχος πρόσβασης.

3.4.27 Δοκιμές και Έλεγχοι Ασφάλειας Εφαρμογών

Διενέργεια δοκιμών και τεχνικών ελέγχων ασφάλειας σε διάφορα στάδια ανάπτυξης των εφαρμογών που η Π.Κ.Μ. αποκτά ή αναπτύσσει, και, σε κάθε περίπτωση, προ της θέσης τους σε παραγωγική λειτουργία.

4. Πολιτική Ορθής Χρήσης Αγαθών και Δεδομένων

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

4.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι η θέσπιση κανόνων για την ορθή, υπεύθυνη και ασφαλή χρήση του εξοπλισμού πληροφορικής, του λογισμικού και των δεδομένων της Περιφέρειας Κεντρικής Μακεδονίας.

4.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε κάθε χρήση πληροφοριακού αγαθού της Π.Κ.Μ. (εξοπλισμός, λογισμικό, ψηφιακές υπηρεσίες και δεδομένα).

4.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την ασφάλεια και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Οργανικών Μονάδων Π.Κ.Μ.:** Υπεύθυνοι για την ενημέρωση και την επιτήρηση των υφισταμένων τους όσον αφορά τη συμμόρφωση τους με τα οριζόμενα στην παρούσα πολιτική.
- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική.

4.4 Αρχές Ορθής Χρήσης Πληροφοριακών Αγαθών και Δεδομένων

Σημ: Ως ΔΔΗΔ αναφέρεται εν συντομία η Διεύθυνση Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Λογαριασμοί Χρηστών:

4.4.1 Απόδοση Διαπιστευτηρίων

Η χρήση του ηλεκτρονικού εξοπλισμού, εφαρμογών, υπηρεσιών και συστημάτων της Π.Κ.Μ. από κάθε χρήστη, επιτρέπεται μόνο έπειτα από τη χορήγηση ενός μοναδικού συνδυασμού Ονόματος Χρήστη (username) και Κωδικού Πρόσβασης (password).

4.4.2 Ευθύνη Επί των Ενεργειών Χρηστών

Όλοι οι χρήστες είναι υπεύθυνοι για τις ενέργειες που πραγματοποιούνται με τα διαπιστευτήριά τους (username & password). Ο διαμοιρασμός και η κοινή χρήση διαπιστευτηρίων δεν επιτρέπονται.

4.4.3 Μη Εξουσιοδοτημένη Πρόσβαση

Δεν επιτρέπεται η πρόσβαση και η απόπειρα πρόσβασης από χρήστες, σε συστήματα ή δεδομένα για τα οποία δεν τους έχουν παραχωρηθεί τα αντίστοιχα δικαιώματα πρόσβασης, λ.χ. πρόσβαση σε:

- Διαχειριστικές λειτουργίες δικτυακών συσκευών και εξυπηρετητών.
- Μη κοινόχρηστα αρχεία σε εξυπηρετητές ή άλλους υπολογιστές.
- Κοινόχρηστα αρχεία και φακέλους Οργανικών Μονάδων σε εξυπηρετητές, χωρίς την έγκριση του εκάστοτε Προϊσταμένου Οργανικής Μονάδας.

Σε περίπτωση εντοπισμού απόπειρας μη εξουσιοδοτημένης πρόσβασης σε λειτουργίες και δεδομένα, διακόπτεται η παροχή κάθε πρόσβασης στον χρήστη, ενημερώνονται οι ιεραρχικά αρμόδιοι και ενεργοποιούνται πειθαρχικές διαδικασίες.

4.4.4 Προστασία Προσωπικών Δεδομένων

Οι χρήστες οφείλουν να δίνουν ιδιαίτερη προσοχή στην αποτροπή μη εξουσιοδοτημένης πρόσβασης σε αρχεία που συμπεριλαμβάνουν δεδομένα προσωπικού χαρακτήρα καθώς και στην αποτροπή διαρροής αυτών. Η πρόσβαση, χρήση και επεξεργασία αρχείων τα οποία συμπεριλαμβάνουν δεδομένα προσωπικού χαρακτήρα πραγματοποιείται βάσει ρητών αρμοδιοτήτων και διαδικασιών που ορίζονται από τον εκάστοτε Προϊστάμενο Οργανικής Μονάδας Π.Κ.Μ.

4.4.5 Αναφορά Διαρροής Κωδικού

Σε περίπτωση κλοπής ή δημοσίευσης του κωδικού πρόσβασης, ο χρήστης υποχρεούται να ειδοποιήσει χωρίς καθυστέρηση τη ΔΔΗΔ.

4.4.6 Διακοπή Πρόσβασης λόγω Παραβάσεων

Σε περίπτωση πραγματοποίησης ενεργειών που παραβαίνουν τα οριζόμενα στην παρούσα πολιτική ή/και στις υπόλοιπες πολιτικές ασφάλειας της Π.Κ.Μ., η ΔΔΗΔ διατηρεί το δικαίωμα να διακόψει την παροχή πρόσβασης σε κάθε υπηρεσία χωρίς προειδοποίηση και να ενημερώσει κάθε ιεραρχικά αρμόδιο.

4.4.7 Μη Γνωστοποίηση Διαπιστευτηρίων

Οι υπάλληλοι της ΔΔΗΔ δεν θα ζητήσουν ποτέ από χρήστη τη γνωστοποίηση των διαπιστευτηρίων του με πρόσχημα την εκτέλεση ενεργειών στον προσωπικό υπολογιστή του η σε κάποια άλλη εφαρμογή – σύστημα. Σε περίπτωση που τρίτο πρόσωπο ζητήσει από χρήστη τη γνωστοποίηση των διαπιστευτηρίων του, ο χρήστης

δεν πρέπει να γνωστοποιήσει τα διαπιστευτήρια του και υποχρεούται να ενημερώσει άμεσα τη ΔΔΗΔ.

Χρήση Η/Υ

4.4.8 Χρήση Μόνο Εγκεκριμένου Λογισμικού

Δεν επιτρέπεται η εγκατάσταση ή χρήση λογισμικού που δεν έχει εγκριθεί από τη ΔΔΗΔ.

4.4.9 Απεγκατάσταση Λογισμικού

Δεν επιτρέπεται η απεγκατάσταση λογισμικού το οποίο έχει εγκατασταθεί από τη ΔΔΗΔ.

4.4.10 Τροποποίηση Ρυθμίσεων Ασφάλειας

Δεν επιτρέπεται η τροποποίηση των ρυθμίσεων ασφάλειας εξοπλισμού, συστημάτων & εφαρμογών και σε περίπτωση εντοπισμού απόπειρας τροποποίησης ρυθμίσεων ασφάλειας, διακόπτεται η παροχή πρόσβασης στον χρήστη, ενημερώνονται οι ιεραρχικά αρμόδιοι και ενεργοποιούνται πειθαρχικές διαδικασίες.

4.4.11 Ακεραιότητα Εξοπλισμού

Ο κάθε χρήστης φροντίζει για την ακεραιότητα του ηλεκτρονικού εξοπλισμού της Π.Κ.Μ ο οποίος έχει διατεθεί σε αυτόν προς χρήση (προσωπικός Η/Υ, οθόνη, λοιπός περιφερειακός εξοπλισμός) καθώς και για τον λοιπό κοινόχρηστο εξοπλισμό (λ.χ. κοινόχρηστοι εκτυπωτές). Ο χρήστης είναι υποχρεωμένος να ενημερώνει τη ΔΔΗΔ σε οποιαδήποτε περίπτωση βλάβης.

4.4.12 Παρέμβαση στον Εξοπλισμό

Απαγορεύεται η οποιαδήποτε επέμβαση στον ηλεκτρονικό εξοπλισμό της Π.Κ.Μ. χωρίς να έχει προηγηθεί επικοινωνία με τη ΔΔΗΔ. Αυτό συμπεριλαμβάνει τη σύνδεση τρίτου υλικού (όπως κάρτες γραφικών ή ήχου) στα συστήματα, καθώς και την αποσύνδεση και μετακίνηση εξαρτημάτων όπως ποντίκια, πληκτρολόγια κλπ.

4.4.13 Αντίγραφα Ασφαλείας Αρχείων Η/Υ

Ο χρήστης μεριμνά για την τακτική λήψη αντιγράφων ασφαλείας των υπηρεσιακών του αρχείων τα οποία είναι αποθηκευμένα στον Η/Υ του. Σε περίπτωση αδυναμίας ή έλλειψης απαραίτητου λογισμικού ή συσκευής λήψης αντιγράφου ασφαλείας θα πρέπει να απευθύνεται εγγράφως στη ΔΔΗΔ. Για τα δεδομένα των εφαρμογών (πχ. Ηλεκτρονικό Πρωτόκολλο, Λογιστική, Διαχείριση Προσωπικού, κτλ.) υπεύθυνη για τη λήψη αντιγράφων ασφαλείας είναι η ΔΔΗΔ.

Χρήση Δικτύου και Ασφάλεια

4.4.14 Σύνδεση Συσκευών στο Δίκτυο της Π.Κ.Μ.

Δεν επιτρέπεται η σύνδεση στο δίκτυο της Π.Κ.Μ., οποιασδήποτε συσκευής δεν έχει εγκριθεί και παραμετροποιηθεί από τη ΔΔΗΔ.

4.4.15 Ορθή Χρήση Δικτυακών Πόρων

Οι χρήστες οφείλουν να μην καταχρώνται τη διαθέσιμη χωρητικότητα των δικτυακών συνδέσεων της Π.Κ.Μ. (λ.χ. μέσω αλόγιστης χρήσης video & radio streaming).

4.4.16 Επίσκεψη Ιστοσελίδων

Οι χρήστες φροντίζουν κατά την επίσκεψη ιστοσελίδων να εφαρμόζουν ιδιαίτερη προσοχή, με σκοπό την αποφυγή μόλυνσης του Η/Υ με κακόβουλο λογισμικό και τη διαρροή διαπιστευτηρίων (λογαριασμοί και κωδικοί χρηστών).

4.4.17 Ενέργειες που Βλάπτουν τη Λειτουργία του Δικτύου

Δεν επιτρέπεται οι χρήστες να διενεργούν πράξεις που έχουν σαν αποτέλεσμα την πρόκληση δυσλειτουργίας στο δίκτυο της Π.Κ.Μ. (λ.χ. μαζική αποστολή email, μαζική λήψη - "κατέβασμα" αρχείων κλπ), χωρίς την ύπαρξη συγκεκριμένου υπηρεσιακού λόγου και την έγκριση της ΔΔΗΔ.

4.4.18 Παράνομο Περιεχόμενο

Δεν επιτρέπεται η απόκτηση ή χρήση/προβολή ή διανομή μέσω του δικτύου της Π.Κ.Μ. περιεχομένου για το οποίο οι χρήστες δεν έχουν νόμιμο δικαίωμα χρήσης (λ.χ. περιπτώσεις που αφορούν πνευματικά δικαιώματα) καθώς και περιεχομένου που με οποιονδήποτε τρόπο παραβιάζει κανόνες δικαίου (λ.χ. παράνομο, συκοφαντικό, απειλητικό, καταχρηστικό, δυσφημιστικό, ρατσιστικό).

4.4.19 Διάθεση Μολυσμένου Περιεχομένου

Οι χρήστες δεν επιτρέπεται να διαθέτουν εν γνώσει τους ή εξαιτίας ενέργειας που παραβιάζει τα οριζόμενα στην παρούσα πολιτική, περιεχόμενο μολυσμένο από κακόβουλο λογισμικό.

5. Πολιτική Αφαιρούμενων Μέσων Αποθήκευσης

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

5.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι η δημιουργία ενός πλαισίου για τη χρήση αφαιρούμενων μέσων, για την ασφαλή αποθήκευση και μεταφορά δεδομένων σε αυτά και την προστασία των υποδομών της Π.Κ.Μ. από κινδύνους που προκύπτουν από τη χρήση μη εξουσιοδοτημένων και πιθανώς μολυσμένων αφαιρούμενων μέσων.

5.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε όλα τα συστήματα της Π.Κ.Μ. στα οποία δύναται να συνδεθούν αφαιρούμενα μέσα καθώς και στο σύνολο των αφαιρούμενων μέσων.

5.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την ασφάλεια και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Οργανικών Μονάδων Π.Κ.Μ.:** Υπεύθυνοι για την έγκριση χρήσης αφαιρούμενων μέσων από τους υφισταμένους τους καθώς και το πλαίσιο που διέπει την αποθήκευση δεδομένων σε αυτά και τη μεταφορά αυτών.
- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική.

5.4 Μέτρα Ασφάλειας

5.4.1 Απαγόρευση Σύνδεσης Αφαιρούμενων Μέσων (Α/Μ)

Εφαρμογή τεχνικών μέτρων για την απαγόρευση της σύνδεσης αφαιρούμενων μέσων σε εξοπλισμό της Π.Κ.Μ., εκτός εάν υπάρχει οργανωτικός ή υπηρεσιακός λόγος για τη χρήση τους.

5.4.2 Έγκριση Χρήσης Α/Μ

Έγκριση χρήσης αφαιρούμενου μέσου από χρήστη μόνο κατόπιν αιτήματος του Προϊσταμένου της αντίστοιχης οργανικής μονάδας προς τη ΔΔΗΔ.

5.4.3 Αποθήκευση Μόνο Εξουσιοδοτημένων Δεδομένων

Μόνο τα δεδομένα που είναι εξουσιοδοτημένα και απαραίτητα για μεταφορά θα πρέπει να αποθηκεύονται σε αφαιρούμενα μέσα. Οι χρήστες πριν χρησιμοποιήσουν αφαιρούμενα μέσα αποθήκευσης λαμβάνουν την έγκριση του Προϊσταμένου τους σχετικά με τα δεδομένα που πρόκειται να μεταφερθούν καθώς και τον προορισμό της μεταφοράς.

5.4.4 Χρήση Εγκεκριμένων Α/Μ

Χρήση μόνο αφαιρούμενων μέσων τα οποία έχει η ΔΔΗΔ διαμοιράσει στους χρήστες.

5.4.5 Καταγραφή και Αναγνωριστικό Α/Μ

Κάθε εξουσιοδοτημένο αφαιρούμενο μέσο φέρει μοναδικό αναγνωριστικό κωδικό και καταγράφεται στον κατάλογο αγαθών πληροφορικής από τη ΔΔΗΔ.

5.4.6 Σήμανση Διαβάθμισης Α/Μ

Στα αφαιρούμενα μέσα αποθήκευσης πρέπει να τοποθετείται σήμανση η οποία θα υποδηλώνει το επίπεδο της διαβάθμισης της πληροφορίας που εμπεριέχεται.

5.4.7 Μη Χρήση Α/Μ για Αρχειοθέτηση

Οι συσκευές αφαιρούμενων μέσων δεν πρέπει να χρησιμοποιούνται για την αρχειοθέτηση ή την αποθήκευση αρχείων ως εναλλακτική λύση έναντι άλλου εξοπλισμό αποθήκευσης.

5.4.8 Προστασία Α/Μ και Δεδομένων

Οι χρήστες ενημερώνονται από τον Προϊστάμενο τους ο οποίος υπέβαλε το αίτημα για χρήση Α/Μ σχετικά με τα οριζόμενα στην παρούσα πολιτική και μεριμνούν για τη φυσική προστασία των αφαιρούμενων συσκευών και των αποθηκευμένων δεδομένων από απώλεια, κλοπή ή ζημία.

5.4.9 Απενεργοποίηση Αυτόματης Εκτέλεσης (Autorun)

Στις περιπτώσεις που η σύνδεση αφαιρούμενων μέσων επιτρέπεται, απενεργοποιείται η αυτόματη εκτέλεση από αυτά.

5.4.10 Αυτόματη Σάρωση για Κακόβουλο Λογισμικό

Στις περιπτώσεις που η σύνδεση αφαιρούμενων μέσων αποθήκευσης επιτρέπεται, τα αφαιρούμενα μέσα σαρώνονται για κακόβουλο λογισμικό, προτού επιτραπεί η χρήση τους.

5.4.11 Κρυπτογράφηση Δεδομένων σε Αφαιρούμενα Μέσα

Κατά περίπτωση, γίνεται χρήση τεχνικών κρυπτογραφίας για την προστασία των δεδομένων σε αφαιρούμενα μέσα αποθήκευσης.

6. Πολιτική Επιχειρησιακής Συνέχειας, Διαχείρισης Περιστατικών και Κρίσεων

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

6.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι ο καθορισμός ενός πλαισίου για τη διατήρηση της επιχειρησιακής συνέχειας, την αντιμετώπιση περιστατικών κυβερνοασφάλειας και τη διαχείριση κρίσεων στην Περιφέρεια Κεντρικής Μακεδονίας, με στόχο την προστασία των κρίσιμων λειτουργιών και πληροφοριακών υποδομών της Π.Κ.Μ. σε περίπτωση διακοπής ή απειλής.

6.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε όλα τα συστήματα πληροφορικής, δίκτυα, υποδομές, δεδομένα, εφαρμογές, και υπηρεσίες που λειτουργούν ή εποπτεύονται από την Π.Κ.Μ.

6.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την ασφάλεια και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική.

6.4 Μέτρα Ασφάλειας

Ανοχή σε Σφάλματα και Επιχειρησιακή Συνέχεια

6.4.1 Σχεδιασμός Ανθεκτικών Συστημάτων

Σχεδιασμός κάθε πληροφοριακού και δικτυακού συστήματος με γνώμονα την ανοχή σε σφάλματα και την υψηλή διαθεσιμότητα, λαμβάνοντας υπόψη την ταξινόμηση του συστήματος όσον αφορά την κρισιμότητα του.

6.4.2 Πλεονασμός / Failover

Χρήση τεχνικών μέτρων όπως ο πλεονασμός υποδομών (redundancy) και η αυτόματη μεταφορά λειτουργιών (failover).

6.4.3 Πλάνο Διασφάλισης Επιχειρησιακής Συνέχειας

Κατάρτιση και τήρηση πλάνου διασφάλισης επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή (Π.Δ.Ε.Σ.Α.Κ), βασισμένο στα αποτελέσματα της διαδικασίας αποτίμησης κινδύνων. Το εν λόγω πλάνο περιλαμβάνει τουλάχιστον τα ακόλουθα:

- Σκοπό και πεδίο εφαρμογής.
- Ρόλους και αρμοδιότητες.
- Σημεία επαφής και κανάλια επικοινωνίας.
- Συνθήκες για την ενεργοποίηση του πλάνου.
- Τη σειρά των ενεργειών ανάκαμψης για συγκεκριμένες λειτουργίες.
- Τους απαιτούμενους πόρους για την ορθή εκτέλεση του πλάνου (λ.χ. πλεονασμός υποδομών).

6.4.4 Ανάλυση επιχειρηματικών επιπτώσεων

Ενσωμάτωση διαδικασίας ανάλυσης επιχειρηματικών επιπτώσεων (business impact analysis) εντός του πλάνου διασφάλισης επιχειρησιακής συνέχεια, με σκοπό την αναγνώριση και αξιολόγηση δυνητικών επιπτώσεων λόγω επέλευσης σοβαρών διαταράξεων στις επιχειρηματικές λειτουργίες της Π.Κ.Μ.

6.4.5 Επαναξιολόγηση Π.Δ.Ε.Σ.Α.Κ

Περιοδική αξιολόγηση και κατά περίπτωση επικαιροποίηση του πλάνου διασφάλισης επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της Π.Κ.Μ. ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.

Διαχείριση περιστατικών κυβερνοασφάλειας

6.4.6 Πλαίσιο Διαχείρισης Περιστατικών

Δημιουργία Πλαισίου Διαχείρισης Περιστατικών Κυβερνοασφάλειας (Π.Δ.Π.Κ), το οποίο καθορίζει τους ρόλους, τις φάσεις και τις διαδικασίες εντοπισμού και απόκρισης.

6.4.7 Ενημέρωση Αρμόδιων Αρχών

Καθορισμός ρόλων και διαδικασιών για την αναφορά περιστατικών στις αρμόδιες αρχές.

6.4.8 Έγκαιρη Αναγνώριση Περιστατικών

Κατάρτιση λεπτομερές πλάνου για την ανίχνευση, ανάλυση και απόκριση σε περιστατικά κυβερνοασφάλειας, καθώς και ανάκαμψης και επαναφοράς των συστημάτων σε ορθή λειτουργία.

6.4.9 Συντονισμός Απόκρισης

Ορισμός τουλάχιστον ενός υπάλληλου ο οποίος θα διαχειρίζεται και συντονίζει τη διαδικασία απόκρισης σε περιστατικά κυβερνοασφάλειας.

6.4.10 Event Logging

Ενεργοποίηση καταγραφής συμβάντων (event logging) σε εξυπηρετητές, δικτυακές συσκευές και Η/Υ χρηστών.

6.4.11 Διατήρηση Αρχείων Καταγραφής

Διατήρηση αρχείων καταγραφής εξυπηρετητών και τειχών προστασίας για προκαθορισμένο χρονικό διάστημα και εφαρμογή επαρκών μέσων προστασίας από μη εξουσιοδοτημένη πρόσβαση και παραποίηση.

6.4.12 Αυτοματοποιημένη Αναγνώριση Περιστατικών

Αξιοποίηση μηχανισμών έγκαιρης αναγνώρισης περιστατικών βάσει εργαλείων καταγραφής, λ.χ εργαλεία Network Monitoring, υπηρεσία S.O.C.

6.4.13 Ενημέρωση DPO σε Συμβάντα

Ενημέρωση του Υπεύθυνου Προστασίας Δεδομένων Π.Κ.Μ. (DPO) σε περίπτωση συμβάντος το οποίο ενδέχεται να επηρεάζει προσωπικά δεδομένα.

6.4.14 Καταγραφή Περιστατικών

Καταγραφής περιστατικών ασφάλειας και τήρησης αρχείων ενεργειών αντιμετώπισης και ενημέρωσης των αρμόδιων αρχών.

6.4.15 Ασκήσεις και Προσομοιώσεις Απόκρισης

Πραγματοποίηση ασκήσεων και προσομοιώσεων για τη δοκιμή των σχεδίων απόκρισης σε κυβερνοεπιθέσεις ή αστοχίες συστημάτων.

6.4.16 Επανεξέταση Π.Δ.Π.Κ.

Περιοδική επανεξέταση του Π.Δ.Π.Κ και επικαιροποίηση εφόσον απαιτείται.

Διαχείριση κρίσεων

6.4.17 Σχέδιο Διαχείρισης Κρίσεων

Κατάρτιση σχεδίου διαχείρισης κρίσεων με προβλεπόμενες ενέργειες επικοινωνίας, λήψης αποφάσεων και συντονισμού κατά τη διάρκεια μείζονος διαταραχής. Το σχέδιο περιλαμβάνει κατ' ελάχιστον:

- Καθορισμό ρόλων και ευθυνών για συγκεκριμένα τμήματα του προσωπικού.
- Καθορισμό των κατάλληλων καναλιών επικοινωνίας με τις αρμόδιες αρχές και το ευρύτερο κοινό, με ιδιαίτερη μέριμνα όσον αφορά στις υποχρεωτικές επικοινωνίες βάσει των νομικών υποχρεώσεων.

6.4.18 Ανασκόπηση και Αξιολόγηση Συμβάντων

Ανασκόπηση συμβάντος μετά από κάθε σοβαρό περιστατικό ή κρίση και αξιολόγηση της αποτελεσματικότητας των ενεργειών που πραγματοποιήθηκαν.

6.4.19 Επαναξιολόγηση Σχεδίου Διαχείρισης Κρίσεων

Περιοδική αξιολόγηση και κατά περίπτωση επικαιροποίηση του σχεδίου διαχείρισης κρίσεων, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της Π.Κ.Μ. ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.

7. Πολιτική Ασφάλειας Εφοδιαστικής Αλυσίδας

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

7.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι η διασφάλιση ότι οι σχέσεις της Περιφέρειας Κεντρικής Μακεδονίας (Π.Κ.Μ.) με προμηθευτές και παρόχους Τεχνολογιών Πληροφορικής και Επικοινωνίων (Τ.Π.Ε.) και εξωτερικούς συνεργάτες, διέπονται από αρχές κυβερνοασφάλειας, ώστε να ελαχιστοποιούνται οι κίνδυνοι που προκύπτουν από την εφοδιαστική αλυσίδα.

7.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε

- Συμβάσεις και συνεργασίες με προμηθευτές προϊόντων Τεχνολογίας Πληροφορικής και Επικοινωνιών (Τ.Π.Ε.).
- Συμβάσεις και συνεργασίες με παρόχους υπηρεσιών (συμπεριλαμβανομένων cloud, hosting, SaaS, τεχνικής υποστήριξης).
- Εξωτερικούς συνεργάτες που έχουν πρόσβαση σε συστήματα, δίκτυα ή δεδομένα της Π.Κ.Μ.

7.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την ασφάλεια και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.

- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική.

7.4 Μέτρα Ασφάλειας

7.4.1 Τεχνικές Προδιαγραφές σε Διαγωνισμούς

Σύνταξη από πλευράς Π.Κ.Μ. των τεχνικών προδιαγραφών που συμπεριλαμβάνονται εντός προσκλήσεων και διαγωνισμών που αφορούν την απόκτηση προϊόντων ή υπηρεσιών Τ.Π.Ε., σύμφωνα με τα οριζόμενα στις πολιτικές ασφάλειας της Π.Κ.Μ.

7.4.2 Μητρώο Κρίσιμων Προμηθευτών

Κατάρτιση καταλόγου άμεσων προμηθευτών και παρόχων υπηρεσιών Τ.Π.Ε., ο οποίος περιλαμβάνει κατ' ελάχιστον:

- Σημεία επαφής, καθώς και τα προϊόντα και υπηρεσίες Τ.Π.Ε. που κάθε προμηθευτής / πάροχος παρέχει.
- Ταξινόμηση των προμηθευτών και παρόχων υπηρεσιών Τ.Π.Ε. σε επίπεδα κρισιμότητας.

7.4.3 Αξιολόγηση Ασφάλειας Αναδόχων

Αξιολόγηση επιπέδου κυβερνοασφάλειας των υποψηφίων προμηθευτών και παρόχων προϊόντων Τ.Π.Ε. λ,χ. βάσει πιστοποιητικών ISO ή ισοδύναμων πιστοποιητικών, πιστοποιήσεων εκτέλεσης έργων κ.τ.λ.), πριν τη σύναψη σύμβασης με αυτούς και λαμβάνοντας παράλληλα υπόψη τη κρισιμότητα του παρεχόμενου προϊόντος ή υπηρεσίας.

7.4.4 Ορισμός Υπεύθυνου Ασφάλειας Αναδόχου

Θέσπιση όρου εντός των συμβάσεων περί ορισμού υπεύθυνου ασφάλειας από την πλευρά των αναδόχων για τη συνεργασία και την επικοινωνία με την Π.Κ.Μ. σε θέματα κυβερνοασφάλειας, όπου αυτό κρίνεται απαραίτητο.

7.4.5 Ρήτρες Ασφάλειας στις Συμβάσεις

Ενσωμάτωση ρητρών ασφάλειας εντός των συμβάσεων Τ.Π.Ε. που συνάπτονται οι οποίες κατ' ελάχιστο ορίζουν την υποχρέωση του αναδόχου για:

- Προστασία δεδομένων και εμπιστευτικότητα.
- Ενσωμάτωση ρητρών ασφάλειας εντός των συμβάσεων Τ.Π.Ε. που συνάπτονται οι οποίες κατ' ελάχιστο ορίζουν την υποχρέωση του αναδόχου για:
- Συμμόρφωση με την ισχύουσα Νομοθεσία περί κυβερνοασφάλειας.
- Άμεση ενημέρωση της Π.Κ.Μ. σε περίπτωση εμφάνισης σοβαρού περιστατικού κυβερνοασφάλειας στις υποδομές του αναδόχου, σε περιπτώσεις αναδόχων που παρέχουν υπηρεσίες Τ.Π.Ε. στην Π.Κ.Μ.
- Άμεση ενημέρωση της Π.Κ.Μ. σε περιπτώσεις εμφάνισης ευπάθειας σε παρεχόμενο από τον ανάδοχο λογισμικό.

8. Πολιτική Ασφάλειας Δικτύων

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

8.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι να προσδιορίσει το γενικό πλαίσιο διαχείρισης της ασφάλειας των δικτύων της Περιφέρειας Κεντρικής Μακεδονίας (Π.Κ.Μ.), ώστε να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών και υπηρεσιών της.

8.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε όλα τα δίκτυα, υποδίκτυα, διασυνδέσεις, συσκευές, υπηρεσίες και υποδομές που ανήκουν στην Π.Κ.Μ. ή τελούν υπό την εποπτεία της. Αφορά όλους τους τελικούς χρήστες, υπαλλήλους, προμηθευτές, τρίτους συνεργάτες και φορείς με εξουσιοδοτημένη ή απομακρυσμένη πρόσβαση.

8.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την ασφάλεια και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική.

8.4 Μέτρα Ασφάλειας

8.4.1 Χρήση Τειχών Προστασίας

Χρήση τειχών προστασίας (firewalls) που περιορίζουν και φιλτράρουν τις δικτυακές συνδέσεις, για την προστασία του δικτύου της Π.Κ.Μ. από μη εξουσιοδοτημένη πρόσβαση.

8.4.2 Αρχιτεκτονική Defense in Depth

Εφαρμογή αρχιτεκτονικής ασφάλειας βάσει της αρχής Άμυνας σε Βάθος (Defense in Depth). Η περίμετρος των δικτύων προστατεύεται μέσω συστημάτων ελέγχου πρόσβασης και φιλτραρίσματος (firewalls ή router access lists). Όλοι οι εξυπηρετητές και σταθμοί εργασίας προστατεύονται με τοπικούς μηχανισμούς firewall (host-based firewall), οι οποίοι είναι παραμετροποιημένοι βάσει του ρόλου της συσκευής.

8.4.3 Διακριτές Δικτυακές Ζώνες

Διαχωρισμός δικτύου σε διακριτά υποδίκτυα ή ζώνες όπου αυτό απαιτείται και φιλτράρισμα της δικτυακής κίνησης μεταξύ των διακριτών υποδικτύων, με βάση τις απαιτήσεις ασφάλειας κάθε ζώνης.

8.4.4 Ελάχιστη Απαραίτητη Επικοινωνία

Ελαχιστοποίηση της επιφάνειας έκθεσης μέσω περιορισμού των προσβάσιμων θυρών, υπηρεσιών και πρωτοκόλλων μόνο στα απολύτως απαραίτητα, σε εξυπηρετητές και σταθμούς εργασίας.

8.4.5 Κατάλογος Επιτρεπόμενων Δικτυακών Ροών

Τήρηση καταλόγου επιτρεπόμενων δικτυακών ροών (Network Flow Inventory) στον οποίο καταγράφονται: πηγές, προορισμοί, πρωτόκολλα και θύρες, υπεύθυνος για τη διαχείριση του πληροφοριακού αγαθού που οι ροές αφορούν, ημερομηνία έγκρισης των ροών και λόγος/ανάγκη για την κάθε ροή.

8.4.6 Τεκμηρίωση και Αίτηση Δικτυακών Ροών

Οι υπεύθυνοι διαχείρισης εφαρμογών, εξυπηρετητών ή υποδομών υποχρεούνται να τεκμηριώνουν τις απαραίτητες θύρες, πρωτόκολλα και κατευθύνσεις ροών δικτύου, οι οποίες είναι απολύτως απαραίτητες για τη λειτουργία των αντίστοιχων υπηρεσιών και να αιτούνται προς τους διαχειριστές του δικτύου Π.Κ.Μ. την υλοποίηση των σχετικών ροών στις συσκευές firewall των κτηρίων της Π.Κ.Μ.

8.4.7 Παραμετροποίηση host-based firewall

Οι υπεύθυνοι διαχείρισης εφαρμογών, εξυπηρετητών ή υποδομών είναι υπεύθυνοι για την παραμετροποίηση του τείχους προστασίας σε επίπεδο host (host-based firewall), για τα συστήματα τα οποία διαχειρίζονται. Σε περιπτώσεις που το host-based firewall είναι κεντρικά διαχειριζόμενο, θα αποστέλλουν σχετικό αίτημα με τις προς υλοποίηση δικτυακές ροές, προς τον διαχειριστή της κεντρικής υπηρεσίας διαχείρισης του host-based firewall.

8.4.8 Απομακρυσμένη Πρόσβαση

Υλοποίηση απομακρυσμένης πρόσβασης σε συστήματα της Π.Κ.Μ. μόνο μέσω κρυπτογραφημένης επικοινωνίας.

8.4.9 Προστασία Διαθεσιμότητας

Προστασία της διαθεσιμότητας κρίσιμων υπηρεσιών, με τεχνικά μέτρα ανθεκτικότητας σε επιθέσεις (π.χ. anti-DDoS) και ύπαρξη εναλλακτικών γραμμών δικτύου.

8.4.10 Περιοδική Αξιολόγηση Πολιτικής και Μέτρων Δικτύου

Περιοδική αξιολόγηση και κατά περίπτωση επικαιροποίηση των μέτρων ασφάλειας δικτύου, ιδίως μετά από σοβαρά περιστατικά ή μεταβολές σε διεθνές επίπεδο απειλών.

9. Πολιτική Διαχείρισης Κινδύνων και Παρακολούθησης Συμμόρφωσης

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

9.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι ο καθορισμός ενός πλαισίου για τη διαχείριση κινδύνων κυβερνοασφάλειας, την παρακολούθηση της συμμόρφωσης, τη διενέργεια ελέγχων και την ασφάλεια της εφοδιαστικής αλυσίδας στην Περιφέρεια Κεντρικής Μακεδονίας. Στόχος της είναι η δημιουργία δομημένων διαδικασιών για την αναγνώριση, αξιολόγηση, αντιμετώπιση και έλεγχο των κινδύνων που απειλούν την ασφάλεια των πληροφοριακών συστημάτων της Π.Κ.Μ.

9.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε όλα τα συστήματα πληροφορικής, δίκτυα, υποδομές, δεδομένα, εφαρμογές, και υπηρεσίες που λειτουργούν ή εποπτεύονται από την Π.Κ.Μ., τις συμβάσεις προμηθειών και υποστήριξης Τεχνολογιών Πληροφοριών και Επικοινωνιών (Τ.Π.Ε.) και τους προμηθευτές / παρόχους Τ.Π.Ε.

9.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την ασφάλεια και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική.

9.4 Μέτρα Ασφάλειας

Διαχείριση και Γνωστοποίηση Ευπαθειών

9.4.1 Εντοπισμός Τεχνικών Ευπαθειών

Υλοποίηση διαδικασιών για τον εντοπισμό, την αξιολόγηση και αντιμετώπιση των τεχνικών ευπαθειών στα συστήματα δικτύου και πληροφοριών της Π.Κ.Μ.

9.4.2 Συλλογή Πληροφοριών Ευπαθειών

Λήψη σε τακτική βάση, πληροφοριών που αφορούν σε τεχνικές ευπάθειες τεχνολογιών πληροφορικής και επικοινωνιών μέσω κατάλληλων πηγών, όπως είναι αρμόδιες αρχές, ερευνητικοί οργανισμοί, προμηθευτές και πάροχοι υπηρεσιών, καθώς και αρμόδιες ομάδες απόκρισης σε περιστατικά κυβερνοασφάλειας (CSIRTs).

9.4.3 Εγκατάσταση Ενημερώσεων Ασφαλείας

Εγκατάσταση ενημερώσεων ασφάλειας (security patches) στα συστήματα δικτύου και πληροφοριών εντός εύλογου χρονικού διαστήματος αφότου αυτές καταστούν διαθέσιμες, με προτεραιοποίηση της εγκατάστασης ιδίως σε συστήματα τα οποία είναι προσβάσιμα με δημόσια IP διεύθυνση μέσω διαδικτύου.

9.4.4 Δοκιμές Ενημερώσεων Ασφαλείας

Διενέργεια δοκιμών των ενημερώσεων ασφάλειας σε ελεγχόμενο περιβάλλον, προτού αυτές εγκατασταθούν σε συστήματα που βρίσκονται σε παραγωγική λειτουργία, εφόσον αυτό κρίνεται απαραίτητο.

9.4.5 Περιοδική Σάρωση Ευπαθειών

Διενέργεια σαρώσεων για ευπάθειες (vulnerability scanning) στα συστήματα δικτύου και πληροφοριών σε περιοδική βάση, μέσω αυτοματοποιημένων εργαλείων, τα αποτελέσματα των οποίων καταγράφονται σε αναλυτική αναφορά.

9.4.6 Αποκατάσταση Ανιχνευμένων Ευπαθειών

Αποκατάσταση των ευπαθειών που έχουν ανιχνευθεί στα συστήματα δικτύου και πληροφοριών εντός εύλογου χρονικού διαστήματος, λαμβάνοντας υπόψη τη σοβαρότητα των ευπαθειών, τις δυνητικές επιπτώσεις τους, καθώς και τη κρισιμότητα των εμπλεκομένων πληροφοριακών αγαθών και δεδομένων.

9.4.7 Τεκμηρίωση Μη Αποκατάστασης Ευπαθειών

Σε περιπτώσεις όπου έχει αποφασισθεί η μη αποκατάσταση μίας ευπάθειας (λ.χ. μη απομονωμένα συστήματα με παράλληλη αδυναμία αναβάθμισης, σχέση κόστους αποκατάστασης με τη πιθανότητα αξιοποίησης της ευπάθειας και τις δυνητικών επιπτώσεις σε περίπτωση αξιοποίησης αυτής), τηρείται κατάλογος με πλήρη τεκμηρίωση για τους λόγους περί μη αποκατάστασης της ευπάθειας.

Αξιολόγηση της αποτελεσματικότητας μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας

9.4.8 Έλεγχοι Αποτελεσματικότητας Μέτρων

Διενέργεια ελέγχων κυβερνοασφάλειας στα συστήματα δικτύου και πληροφοριών , για το σκοπό της αξιολόγησης της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας που έχουν υλοποιηθεί σε αυτά.

9.4.9 Εξωτερικά Penetration Tests

Διενέργεια εξωτερικών ελέγχων παρείσδυσης (external penetration tests) στα συστήματα δικτύου και πληροφοριών της Π.Κ.Μ. που είναι προσβάσιμα από το

διαδίκτυο, σε περιοδική βάση και τουλάχιστον μία φορά ετησίως ή κατόπιν σοβαρού περιστατικού κυβερνοασφάλειας.

9.4.10 Εσωτερικά Penetration Tests

Διενέργεια εσωτερικών ελέγχων παρείσδυσης (internal penetration tests) στα συστήματα δικτύου και πληροφοριών της Π.Κ.Μ., με βάση το σχήμα ταξινόμησης των αγαθών και των δεδομένων.

9.4.11 Αποκατάσταση Ευρημάτων Ελέγχων

Υλοποίηση πλάνου αποκατάστασης των ελλείψεων που διαπιστώνονται από εξωτερικούς και εσωτερικού έλεγχους παρείσδυσης με προτεραιοποίηση βάσει της κρισιμότητας των ευρημάτων.

9.4.12 Ετήσια Αυτοαξιολόγηση Ασφάλειας

Διενέργεια σε ετήσια βάση ή κατόπιν σοβαρού περιστατικού κυβερνοασφάλειας, αυτοαξιολόγηση της ασφάλειας των συστημάτων δικτύου και πληροφοριών της Π.Κ.Μ., με χρήση κατάλληλου Οδηγού που εκδίδει και αναθεωρεί η Εθνική Αρχή Κυβερνοασφάλειας. Τα αποτελέσματά της αυτοαξιολόγησης αποστέλλονται στην Εθνική Αρχή Κυβερνοασφάλειας, συνοδευόμενα από πλάνο διορθωτικών ενεργειών.

Πλαίσιο Διαχείριση Κινδύνων Κυβερνοασφάλειας

9.4.13 Πλαίσιο Διαχείρισης Κινδύνων

Διαμόρφωση και εφαρμογή κατάλληλου Πλαισίου Διαχείρισης των Κινδύνων Κυβερνοασφάλειας (ΠΔΚΚ), το οποίο ευθυγραμμίζεται με τα τα μέτρα και τις διαδικασίες που υλοποιούνται βάσει της παρούσας και των υπολοίπων πολιτικών ασφάλειας της Π.Κ.Μ.

9.4.14 Risk Assesment

Διενέργεια εκτίμησης κινδύνων (risk assessment) σε περιοδική βάση, με την εφαρμογή μεθοδολογιών που βασίζονται σε διεθνή πρότυπα ή/και βέλτιστες πρακτικές, λαμβάνοντας επίσης υπόψη:

- Πληροφορίες που αφορούν σε κυβερνοαπειλές (cyber threat intelligence) από αξιόπιστες και τεχνικά εξειδικευμένες πηγές.
- Τα αποτελέσματα αξιολόγησης των ευπαθειών στα συστήματα δικτύου και πληροφοριών της Π.Κ.Μ.

9.4.15 Risk treatment plan

Ανάπτυξη και υλοποίηση πλάνου αντιμετώπισης των κινδύνων κυβερνοασφάλειας (risk treatment plan) όπου στην επιλογή και προτεραιοποίηση των τεχνικών, οργανωτικών και επιχειρησιακών μέτρων αντιμετώπισης των κινδύνων, λαμβάνονται υπόψη:

- Το σχήμα ταξινόμησης των αγαθών και των δεδομένων.
- Τα αποτελέσματα της ανάλυσης επιχειρηματικών επιπτώσεων.
- Τα αποτελέσματα της διαδικασίας αξιολόγησης της αποτελεσματικότητας των μέτρων διαχείρισης των κινδύνων κυβερνοασφάλειας.
- Τα αποτελέσματα της διαδικασίας εκτίμησης κινδύνων.
- Το κόστος υλοποίησης σε σχέση με το προσδοκώμενο όφελος.

Ανεξάρτητος έλεγχος ασφάλειας πληροφοριών & Διαδικασίες παρακολούθησης της συμμόρφωσης

9.4.16 Ανεξάρτητοι Έλεγχοι

Υλοποίηση ανεξάρτητων ελέγχων (independent audits) του συνόλου των παραμέτρων του προγράμματος διαχείρισης ασφάλειας πληροφοριών της Π.Κ.Μ., συμπεριλαμβανομένων του προσωπικού, των πολιτικών, των διαδικασιών και των τεχνολογιών που χρησιμοποιούνται, σε περιοδική βάση καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας. Οι εν λόγω έλεγχοι δύνανται να διενεργούνται από εσωτερικούς ή εξωτερικούς ελεγκτές και πρέπει να διασφαλίζεται η αμεροληψία αυτών.

9.4.17 Διορθωτικές Ενέργειες

Εκκίνηση διαδικασιών διορθωτικών ενεργειών σε περίπτωση που από τα αποτελέσματα του ανεξάρτητου ελέγχου προκύψει ανεπαρκής υλοποίηση των απαραίτητων τεχνικών, οργανωτικών και επιχειρησιακών μέτρων κυβερνοασφάλειας.

9.4.18 Παρακολούθηση Συμμόρφωσης

Υλοποίηση διαδικασίων παρακολούθησης και αξιολόγησης της συμμόρφωσής της Π.Κ.Μ. με τις κανονιστικές της υποχρεώσεις που σχετίζονται με την κυβερνοασφάλεια, σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα μεταβολές στο σχετικό κανονιστικό πλαίσιο

9.4.19 Διορθωτικές Ενέργειες Συμμόρφωσης

Εκκίνηση διαδικασιών διορθωτικών ενεργειών σε περίπτωση που από τα αποτελέσματα των διαδικασιών παρακολούθησης και αξιολόγησης της συμμόρφωσής της Π.Κ.Μ. με τις κανονιστικές της υποχρεώσεις που σχετίζονται με την κυβερνοασφάλεια, προκύψει ανεπαρκής συμμόρφωση.

10. Πολιτική Αντιγράφων Ασφάλειας

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

10.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι ο καθορισμός των κανόνων και των διαδικασιών που ακολουθεί η Περιφέρεια Κεντρικής Μακεδονίας (Π.Κ.Μ.) για τη δημιουργία, αποθήκευση, διατήρηση και έλεγχο αντιγράφων ασφαλείας (backups) δεδομένων, εφαρμογών και συστημάτων. Η πολιτική αυτή διασφαλίζει τη διαθεσιμότητα και την ακεραιότητα των πληροφοριών, καθώς και τη δυνατότητα άμεσης αποκατάστασης της λειτουργίας σε περίπτωση περιστατικού κυβερνοασφάλειας, φυσικής καταστροφής ή ανθρώπινου λάθους.

10.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε όλους τους εξυπηρετητές (φυσικούς και εικονικούς), σε βάσεις δεδομένων, εφαρμογές και αρχεία αναλόγως με την ταξινόμηση της κρισιμότητας του κάθε ενός εκ των παραπάνω πληροφοριακών αγαθών και αφορά όλα τα είδη αντιγράφων ασφαλείας ((πλήρη, διαφορικά, αυξητικά).

10.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την ασφάλεια και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας

Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική.

10.4 Μέτρα Ασφάλειας

10.4.1 Διαδικασίες Λήψης Αντιγράφων Ασφαλείας

Υλοποίηση διαδικασίων που αφορούν τη λήψη και ασφαλή διαχείριση των αντιγράφων ασφαλείας (backups) συστημάτων, εφαρμογών και δεδομένων.

10.4.2 Αυτόματη Λήψη Αντιγράφων Ασφαλείας

Λήψη και τήρηση αντιγράφων ασφαλείας συστημάτων, εφαρμογών και δεδομένων με αυτοματοποιημένο τρόπο, λαμβάνοντας υπόψη την ταξινόμηση της κρισιμότητάς τους.

10.4.3 Πρόγραμμα Λήψης Αντιγράφων Ασφαλείας

Καθορισμός τακτικού προγράμματος λήψης αντιγράφων ασφαλείας για όλα τα κρίσιμα συστήματα.

10.4.4 Καθημερινός Έλεγχος Αντιγράφων

Καθημερινός έλεγχος της επιτυχίας λήψης αντιγράφων ασφάλειας και τήρηση αποτελεσματών σε ειδικό αρχείο.

10.4.5 Χρονική Διατήρηση Αντιγράφων

Διατήρηση των αντιγράφων ασφαλείας για συγκεκριμένο χρονικό διάστημα ανάλογα με την κατηγορία των δεδομένων και τις εκάστοτε κανονιστικές απαιτήσεις.

10.4.6 Πρόσβαση στα Αντίγραφα Ασφάλειας

Υλοποίηση κατάλληλων μέτρων για τον έλεγχο της φυσικής και λογικής πρόσβασης στα αντίγραφα ασφαλείας, σε αντιστοιχία με το σχήμα ταξινόμησης των αγαθών και των δεδομένων.

10.4.7 Αποθήκευση σε Διαφορετικά Μέσα & Off-Site

Αποθήκευση αντιγράφων ασφάλειας σε τουλάχιστον δύο διαφορετικά μέσα αποθήκευσης, εκ των οποίων το ένα βρίσκεται εκτός της κύριας τοποθεσίας (off-site).

10.4.8 Πρόσβαση Εξουσιοδοτημένων Χρηστών

Απόδοση πρόσβασης στα αντίγραφα ασφάλειας μόνο σε εξουσιοδοτημένους χρήστες.

10.4.9 Κρυπτογράφηση Αντιγράφων

Κρυπτογράφηση των αντιγράφων ασφάλειας κατά την μεταφορά (in-transit) και κατά την αποθήκευση (in-rest).

10.4.10 Δοκιμές Επαναφοράς Αντιγράφων Ασφάλειας

Υλοποίηση δοκιμών επαναφοράς (restoration) επιλεγμένου δείγματος των αντιγράφων ασφαλείας σε περιοδική βάση.

11. Πολιτική Κρυπτογράφησης Δεδομένων και Επικοινωνιών

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

11.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι ο καθορισμός ενός πλαισίου για την κρυπτογράφηση δεδομένων και επικοινωνιών στην Περιφέρεια Κεντρικής Μακεδονίας (Π.Κ.Μ.), ώστε να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα των πληροφοριών.

11.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται στο σύνολο των δεδομένων, υποδομών, συστημάτων, υπηρεσιών, εφαρμογών αφαιρούμενων μέσων και στο σύνολο της δικτυακής επικοινωνίας (εσωτερικής και εξωτερικής).

11.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την ασφάλεια και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική.

11.4 Μέτρα Ασφάλειας

Κρυπτογράφηση Δεδομένων σε Ανάπαυση (Encryption at Rest)

11.4.1 Υλοποίηση Διαδικασιών Κρυπτογράφησης

Υλοποίηση διαδικασίων που αφορούν στην κρυπτογραφία, με σκοπό τη διασφάλιση της εμπιστευτικότητας, αυθεντικότητας και ακεραιότητας των δεδομένων της Π.Κ.Μ., σε συμφωνία με το σχήμα ταξινόμησης των αγαθών και των δεδομένων, καθώς και τα αποτελέσματα της αποτίμησης επικινδυνότητας.

11.4.2 Encryption at Rest

Κρυπτογράφηση των δεδομένων που έχουν ταξινομηθεί ως αυξημένης κρισιμότητας και είναι αποθηκευμένα σε Η/Υ τελικού χρήστη, διακομιστές, αφαιρούμενα μέσα, εφαρμογές και βάσεις δεδομένων (encryption at rest), όπου αυτό κρίνεται απαραίτητο και είναι τεχνικά εφικτό.

11.4.3 Encryption in Transit

Κρυπτογράφηση των δεδομένων που έχουν ταξινομηθεί ως αυξημένης κρισιμότητας, κατά τη μεταφορά τους μέσω του δικτύου.

11.4.4 Κρυπτογράφηση Διαπιστευτηρίων

Αποθήκευση κωδικών πρόσβασης εντός των πληροφοριακών συστημάτων που υλοποιούν διαδικασίες αυθεντικοποίησης αποκλειστικά σε μη αναστρέψιμη, κρυπτογραφικά ασφαλή μορφή, με τη χρήση κατάλληλων συναρτήσεων κατακερματισμού (hash functions). Δεν επιτρέπεται η αποθήκευση κωδικών σε απλό κείμενο (plaintext).

11.4.5 Επιλογή Μεθόδου Κρυπτογράφησης

Η τεχνική μέθοδος και το επίπεδο κρυπτογράφησης επιλέγονται αναλόγως του επιπέδου προστασίας και και του σχήματος ταξινόμησης των αγαθών και των δεδομένων

11.4.6 Διαχείριση Κρυπτογραφικών Κλειδιών

Υλοποίηση διαδικασιών για την προσέγγιση στη διαχείριση των κρυπτογραφικών κλειδιών και ψηφιακών πιστοποιητικών, συμπεριλαμβανομένων των μεθόδων δημιουργίας, διανομής, αποθήκευσης, αλλαγής και ανάκλησής τους.

11.4.7 Περιοδική Αναθεώρηση Κρυπτογράφησης

Περιοδική αξιολόγηση και κατά περίπτωση επικαιροποίηση των διαδικασίων που αφορούν στην κρυπτογραφία λαμβάνοντας υπόψη τις εξελίξεις στις μεθόδους και τεχνολογίες κρυπτογράφησης.

12. Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικού πλαισίου κυβερνοασφάλειας

12.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι ο καθορισμός ενός πλαίσιου για τη φυσική και περιβαλλοντική ασφάλεια των εγκαταστάσεων της Περιφέρειας Κεντρικής Μακεδονίας (Π.Κ.Μ.) και των πληροφοριακών της υποδομών, με στόχο την προστασία από μη εξουσιοδοτημένη φυσική πρόσβαση, την αποτροπή περιβαλλοντικών και φυσικών απειλών και τη διασφάλιση της συνεχούς λειτουργίας των πληροφοριακών συστημάτων.

12.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε όλους τους χώρους και εγκαταστάσεις της Π.Κ.Μ. που φιλοξενούν πληροφοριακά συστήματα ή εξοπλισμό πληροφορικής.

12.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την ασφάλεια και ορθή λειτουργία των πληροφοριακών συστημάτων της Π.Κ.Μ. και των πληροφοριών που διακινούνται σε αυτά.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής καθώς και την επικοινωνία με τις αρμόδιες αρχές στις περιπτώσεις που αυτό είναι απαραίτητο.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για τον περιοδικό έλεγχο της εφαρμογής των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εφαρμογή των τεχνικών μέτρων και των διαδικασιών ασφάλειας που αφορούν τα πληροφοριακά συστήματα της Π.Κ.Μ, όπως προβλέπονται στην παρούσα πολιτική.
- **Τελικοί χρήστες:** Οι υπάλληλοι της Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών ή οποιοδήποτε φυσικό ή νομικό πρόσωπο αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική.

12.4 Μέτρα Ασφάλειας

12.4.1 Μέτρα Φυσικής Ασφάλειας

Υλοποίηση επαρκών μέτρων φυσικής ασφάλειας και επίβλεψης στην περίμετρο των εγκαταστάσεών της Π.Κ.Μ., καθώς και, όπου απαιτείται, εσωτερικές διακριτές ζώνες προστασίας ανάλογες με τις απαιτήσεις ασφάλειας κάθε ζώνης.

12.4.2 Φυσικός Έλεγχος Πρόσβασης

Η φυσική πρόσβαση στους χώρους που φιλοξενούν κρίσιμα πληροφοριακά συστήματα της Π.Κ.Μ. περιορίζεται σε εξουσιοδοτημένο προσωπικό με την εφαρμογή κατάλληλων μεθόδων ταυτοποίησης, καταγραφής και επίβλεψης.

12.4.3 Προστασία από Φυσικούς & Περιβαλλοντικούς Κινδύνους

Υλοποίηση επαρκών μέτρων προστασίας από φυσικούς και περιβαλλοντικούς κινδύνους, ιδίως όσον αφορά στις περιπτώσεις πυρκαγιάς, πλημμύρας και εγκληματικής δραστηριότητας.

12.4.4 Προστασία από Αστοχίες

Υλοποίηση επαρκών μέτρων προστασίας και επίβλεψης των μηχανισμών και μέσων υποστήριξης της συνεχούς λειτουργίας των πληροφοριακών συστημάτων της Π.Κ.Μ., ιδίως όσον αφορά στα μέσα παροχής ηλεκτρισμού, νερού, εξαερισμού και κλιματισμού, από συμβάντα αστοχίας ή σοβαρής διατάραξης της λειτουργίας τους.

12.4.5 Περιοδική Αναθεώρηση Πολιτικών

Η πολιτική και οι διαδικασίες φυσικής και περιβαλλοντικής ασφάλειας αξιολογούνται και, κατά περίπτω- ση, επικαιροποιούνται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά φυσικής και περιβαλλοντικής ασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας.

13. Πολιτική Ασφάλειας & Εκπαίδευσης Ανθρώπινου Δυναμικού

Η παρούσα πολιτική δεν περιλαμβάνει ευαίσθητες τεχνικές πληροφορίες, οι οποίες τηρούνται σε εσωτερικές διαδικασίες της Διεύθυνσης Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.

Έκδοση	Συντάκτης	Εγκρίθηκε από	Ημ/νια Έγκρισης	Αναθεώρηση Εγγράφου
1.0	Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.	Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας		➢ Σε περιπτώσεις που προκύπτει η ανάγκη προσθήκης / τροποποίησης στοιχείων. ➢ Μετά από εμφάνιση σοβαρού περιστατικού. ➢ Κατόπιν αλλαγής του νομικού και κανονιστικό πλαισίου κυβερνοασφάλειας

13.1 Σκοπός

Η παρούσα πολιτική εντάσσεται στο Ολοκληρωμένο Πρόγραμμα Διαχείρισης Κινδύνων Κυβερνοασφάλειας της Π.Κ.Μ., σύμφωνα με την ΚΥΑ 1689/2025. Σκοπός της είναι η διασφάλιση ύπαρξης διαδικασιών για τον έλεγχο των προσόντων του ανθρώπινου δυναμικού και την κατάρτιση αυτού σε θέματα κυβερνοασφάλειας.

13.2 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε όλα τα μέλη του προσωπικού της Π.Κ.Μ. που διαθέτουν πρόσβαση σε δεδομένα ή συστήματα της Π.Κ.Μ.

13.3 Ρόλοι και Ευθύνες

- **Περιφερειακό Συμβούλιο Κεντρικής Μακεδονίας:** Υπεύθυνο για την έγκριση της παρούσας πολιτικής.
- **Αντιπεριφερειάρχης Ψηφιακής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνος για την οργάνωση και υλοποίηση προγραμμάτων ευαισθητοποίησης επί βασικών θεμάτων κυβερνοασφάλειας.
- **Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.):** Υπεύθυνος για την παρακολούθηση της συμμόρφωσης της Π.Κ.Μ. με τις απαιτήσεις της παρούσας πολιτικής στο σκέλος που αφορά τη δημιουργία υλικού εκπαίδευσης και υλοποίηση προγραμμάτων ευαισθητοποίησης επί βασικών θεμάτων κυβερνοασφάλειας.
- **Διεύθυνση Ανθρώπινου Δυναμικού και Διαχείρισης Ποιότητας Π.Κ.Μ.:** Υπεύθυνη για την υλοποίηση διαδικασιών επί της ασφάλειας ανθρώπινου δυναμικού.
- **Διεύθυνση Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνη για την οργάνωση του υλικού εκπαίδευσης και τη συνεργασία με τρίτους (λ.χ. Οργανισμούς και εξειδικευμένες Εταιρείες), όσον αφορά το υλικό εκπαίδευσης και την υλοποίηση προγραμμάτων ευαισθητοποίησης επί βασικών θεμάτων κυβερνοασφάλειας.
- **Προϊστάμενοι Τμημάτων Διεύθυνσης Διαφάνειας & Ηλεκτρονικής Διακυβέρνησης Π.Κ.Μ.:** Υπεύθυνοι για την εξειδίκευση και τον έλεγχο του υλικού εκπαίδευσης καθώς και τη διασφάλιση των τεχνικών προϋποθέσεων για την υλοποίηση των προγραμμάτων ευαισθητοποίησης.
- **Προϊστάμενοι Οργανικών Μονάδων Π.Κ.Μ.:** Υπεύθυνοι για το συνολικό επίπεδο τήρησης των βασικών αρχών κυβερνοασφάλειας από τους υφισταμένους τους καθώς και για την καθοδήγηση/παρότρυνση των υφισταμένων του ως προς την παρακολούθηση στοχευμένων σεμιναρίων, τόσο σε θέματα κυβερνοασφάλειας όσο και γενικών ψηφιακών δεξιοτήτων, όταν διαπιστώνονται ελλείψεις.

- **Τελικοί χρήστες:** Οι υπάλληλοι και εξωτερικοί συνεργάτες που αποκτούν πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας, υποχρεούνται να τηρούν τα οριζόμενα στην παρούσα πολιτική και να διατηρούν το απαραίτητο προσωπικό επίπεδο γνώσεων επί βασικών θεμάτων κυβερνοασφάλειας καθώς και γενικών ψηφιακών δεξιοτήτων.

13.4 Μέτρα Ασφάλειας

Ασφάλεια Ανθρώπινου Δυναμικού

13.4.1 Ενημέρωση Προσωπικού Περί Ευθυνών

Υλοποίηση διαδικασίας ενημέρωσης και δέσμευσης επί των οριζόμενων στις πολιτικές ασφάλειας της Π.Κ.Μ., οποιουδήποτε φυσικού ή νομικού προσώπου αποκτά πρόσβαση σε πληροφοριακά συστήματα, εφαρμογές ή εξοπλισμό της Περιφέρειας Κεντρικής Μακεδονίας (λ.χ. υπάλληλοι Π.Κ.Μ., εξωτερικοί συνεργάτες, τρίτοι προμηθευτές και πάροχοι υπηρεσιών).

13.4.2 Κοινοποίηση Ευθυνών Μετά τη Λήξη Σχέσης Εργασίας

Κοινοποίηση στο αρμόδιο προσωπικό των ευθυνών και καθηκόντων που παραμένουν σε ισχύ μετά τη λήξη της σχέσης εργασίας ή τυχόν αλλαγής της κατάστασης απασχόλησης με την Π.Κ.Μ.

Εκπαίδευση & Ευαισθητοποίηση Ανθρώπινου Δυναμικού

13.4.3 Βασική Εκπαίδευση Κυβερνοασφάλειας

Παροχή βασικής εκπαίδευσης σε θέματα κυβερνοασφάλειας (λ.χ. παροχή εκπαιδευτικού υλικού και τεστ αξιολόγησης γνώσεων), σε κάθε άτομο που συνάπτει σχέση εργασίας με την Π.Κ.Μ., εντός σύντομου χρονικού διαστήματος από την σύναψη σχέσης εργασίας.

13.4.4 Προγράμματα Εκπαίδευσης & Ευαισθητοποίησης

Διενέργεια σε περιοδική βάση, προγραμμάτων εκπαίδευσης και ασκήσεων ευαισθητοποίησης (π.χ. προσομοιωμένες επιθέσεις phishing), στο σύνολο του προσωπικού της Π.Κ.Μ.

13.4.5 Εξειδικευμένα Προγράμματα Εκπαίδευσης

Διενέργεια σε περιοδική βάση, προγραμμάτων εκπαίδευσης σε θέματα κυβερνοασφάλειας για συγκεκριμένες κατηγορίες εργαζομένων, με βάση τον τεχνικά εξειδικευμένο ρόλο και τις αρμοδιότητές τους στη διαχείριση των συστημάτων δικτύου και πληροφοριών της Π.Κ.Μ.