ΠΟΛΙΤΙΚΗ ΔΕΟΝΤΟΛΟΓΙΑΣ / ΟΡΘΗΣ ΚΑΙ ΑΣΦΑΛΟΥΣ ΧΡΗΣΗΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Έκδοση 1η

Ημερομηνία Ενημέρωσης : Οκτώβριος 2024

1. Σκοπός και πεδίο εφαρμογής

1.1. Εισαγωγή

Η Αποκεντρωμένη Διοίκηση Μακεδονίας - Θράκης (Α.Δ.Μ.-Θ.) αναγνωρίζοντας τη σημασία της ασφαλούς χρήσης των Πληροφοριακών Συστημάτων στην αποφυγή διαρροής, απώλειας ή υποβάθμισης των δεδομένων που διαθέτει και χειρίζεται, προτίθεται να εφαρμόσει πολιτική με την οποία να διασφαλίζεται η συμμόρφωση με την σχετική νομοθεσία και να ελαχιστοποιείται ο κίνδυνος για μη εξουσιοδοτημένη πρόσβαση στα πληροφοριακά της συστήματα. Η προστασία των πληροφοριών και των συστημάτων επεξεργασίας τους είναι στρατηγικής σημασίας για την Α.Δ.Μ.-Θ., καθώς καθορίζει σε μέγιστο βαθμό την ομαλή και σύννομη λειτουργία της και την επίτευξη του σκοπού και των στόχων της.

1.2 Σκοπός

Σκοποί της Πολιτικής αυτής είναι οι εξής:

- Η ικανοποίηση των νομοθετικών και κανονιστικών απαιτήσεων.
- Η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που διαχειρίζεται η Α.Δ.Μ.-Θ., περιλαμβανομένων των προσωπικών δεδομένων.
- Η εξασφάλιση της ορθής λειτουργίας των πληροφοριακών συστημάτων μέσω των οποίων παρέχονται υπηρεσίες στους πολίτες και στους υπαλλήλους του φορέα.
- Ο έγκαιρος εντοπισμός και η κατάλληλη αντιμετώπιση περιστατικών που είναι δυνατόν να θέσουν σε κίνδυνο την ασφάλεια των πληροφοριακών συστημάτων και των πληροφοριών.
- Η συνεχής βελτίωση του επιπέδου ασφάλειας των πληροφοριακών συστημάτων και των πληροφοριών.

1.3 Ρόλοι

Χρήστες. Οι χρήστες είναι οι με οποιαδήποτε σχέση εργασίας υπάλληλοι του φορέα καθώς και

οποιοσδήποτε τρίτος μπορεί να έχει πρόσβαση στα πληροφοριακά συστήματα του φορέα είτε στον χώρο εργασίας είτε από απόσταση. Οι χρήστες είναι υπεύθυνοι για την ορθή και ασφαλή χρήση των πληροφοριακών συστημάτων σύμφωνα με την παρούσα πολιτική αλλά και οποιαδήποτε συναφή πολιτική ή οδηγία που εκδίδεται από τον φορέα. Κάθε χρήστης είναι υπεύθυνος για την προστασία των δεδομένων και αρχείων του υπολογιστή του. Για την αποφυγή της απώλειας των υπηρεσιακών δεδομένων, ο χρήστης πρέπει να φροντίζει να κρατά αντίγραφα ασφαλείας σύμφωνα με τις κατευθυντήριες οδηγίες της παρούσας πολιτικής.

Προϊστάμενοι. Οι προϊστάμενοι των οργανικών μονάδων της Α.Δ.Μ.-Θ. μεριμνούν για την εύρυθμη λειτουργία τους εξειδικεύοντας τους στόχους και τον προγραμματισμό της δράσης τους. Στο πλαίσιο της εύρυθμης λειτουργίας είναι αρμόδιοι για τη μετάδοση κάθε αναφοράς για την τήρηση ή μη των κανόνων ορθής χρήσης και δεοντολογίας των πληροφοριακών συστημάτων, όπως αναλύονται στην παρούσα πολιτική.

Διεύθυνση Πληροφορικής και Επικοινωνιών. Η Διεύθυνση Πληροφορικής και Επικοινωνιών μεριμνά για την ασφαλή χρήση και την προστασία των πληροφοριακών συστημάτων αλλά και την ομαλή λειτουργία και προστασία του δικτύου του φορέα από εξωτερικές απειλές. Στο πλαίσιο αυτό είναι αρμόδια για :

- Τον σχεδιασμό, την υλοποίηση και τη διατήρηση μέτρων ασφάλειας των πληροφοριακών συστημάτων.
- Την τακτική παρακολούθηση και αξιολόγηση των κινδύνων ασφάλειας των πληροφοριακών συστημάτων.
- Την αντιμετώπιση και διαχείριση περιστατικών ασφάλειας.
- Τον προσδιορισμό ασφαλών μεθόδων απομακρυσμένης πρόσβασης στο ενσύρματο και ασύρματο δίκτυο του φορέα.
- Τη διατήρηση κύριων λιστών δικαιωμάτων πρόσβασης και διαχειριστών πρόσβασης.

Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.) Σύμφωνα με το άρθρο 18 του Ν. 4961 (ΦΕΚ 146/Α΄/2022) ο ΥΑΣΠΕ που έχει ως κύριο καθήκον την παρακολούθηση της θωράκισης του φορέα από κυβερνοαπειλές με σκοπό την επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας.

Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ). Σύμφωνα με το άρθρο 39 παράγραφος 1 στοιχείο β) του Κανονισμού (ΕΕ) 2016/679, ο ΥΠΔ έχει ως κύριο καθήκον την παρακολούθηση της συμμόρφωσης με τον Γενικό Κανονισμό Προστασίας Δεδομένων.
Στο πλαίσιο των καθηκόντων παρακολούθησης της συμμόρφωσης, ο ΥΠΔ προβαίνει στις εξής ενέργειες:

- συλλέγει πληροφορίες με σκοπό τον προσδιορισμό δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων,
- αναλύει και ελέγχει τη συμμόρφωση των δραστηριοτήτων επεξεργασίας,
- ενημερώνει τη διοίκηση του φορέα για τις υποχρεώσεις που απορρέουν από τον Κανονισμό,

παρέχει συμβουλές και εκδίδει συστάσεις όταν απαιτείται.
- λειτουργεί ως σημείο επικοινωνίας με την εποπτική αρχή (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα).

1.4 Εύρος εφαρμογής

Η πολιτική ασφάλειας αφορά όλα τα πληροφοριακά συστήματα, τα υπολογιστικά συστήματα και τον ψηφιακό εξοπλισμό, τους προσωπικούς και φορητούς Η/Υ, τους εξυπηρετητές, εκτυπωτές, σαρωτές, το λογισμικό, τις υπηρεσίες και εφαρμογές δικτύου και διαδικτύου, τις βάσεις δεδομένων και λοιπά πληροφοριακά συστήματα, τις ηλεκτρονικές σελίδες, το δίκτυο (ενσύρματο και ασύρματο), το τηλεφωνικό δίκτυο και τις συσκευές αυτού και το υπηρεσιακό ηλεκτρονικό ταχυδρομείο. Η πολιτική αυτή έχει υποχρεωτικό χαρακτήρα για όλους τους χρήστες Πληροφοριακών Συστημάτων του φορέα.

Η πολιτική αυτή εφαρμόζεται σε :

- εξοπλισμό και συστήματα που χρησιμοποιούν μόνιμα ή προσωρινά τη δικτύωση και τους πόρους των πληροφοριακών συστημάτων της Α.Δ.Μ.-Θ., είτε παρέχονται από τον φορέα είτε είναι ιδιωτικά.
- οποιαδήποτε άλλα συστήματα τα οποία αποκτούν, εξουσιοδοτημένη ή μη, σύνδεση & πρόσβαση στο δίκτυο της Α.Δ.Μ-Θ.
- σε υπολογιστικά συστήματα ή κινητές συσκευές που διατηρούνται ή χρησιμοποιούνται εκτός των χώρων της Α.Δ.Μ.-Θ. και των γραμμών ΣΥΖΕΥΞΙΣ από υπαλλήλους της Α.Δ.Μ.-Θ. που συνδέονται εξ αποστάσεως με το δίκτυο, τα πληροφοριακά συστήματα ή τις υπηρεσίες της Α.Δ.Μ.-Θ. .

2. Νομικό Πλαίσιο και βασικές αρχές

2.1 Νομοθεσία

Η Πολιτική έλαβε υπόψη τις οδηγίες της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - Εθνικό CERT, τον **Ν.3528/2007** (Υπαλληλικός Κώδικας) , τον **Ν. 4411/2016** (Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και άλλες διατάξεις.), τον **Ν. 3471/06** (Προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών), τον **Ν.4961/2022** (Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις), τον **Κανονισμό (ΕΕ) 2016/679** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Γενικός Κανονισμός για την Προστασία Δεδομένων - GDPR), τον Ν. **4624/2019** (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679) , τον **Ν.4727/20 (**Ψηφιακή

Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024 - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972), τον **Κώδικα Επικοινωνίας Δημοσίων Υπηρεσιών,** τον **Κώδικα Ηθικής και Επαγγελματικής Συμπεριφοράς Υπαλλήλων του Δημόσιου Τομέα**, **το Εγχειρίδιο Κυβερνοασφάλειας** της Εθνικής Αρχής Κυβερνοασφάλειας και την **Εθνική Στρατηγική Κυβερνοασφάλειας 2020 – 2025** όπως τροποποιήθηκαν και ισχύουν.

2.2 Βασικές Αρχές

Οι βασικές αρχές που διέπουν τη χρήση των πληροφοριακών συστημάτων της Α.Δ.Μ.-Θ. από τους τελικούς χρήστες συνοψίζονται στα εξής:

- Η χρήση των συστημάτων πληροφορικής και επικοινωνιών της Α.Δ.Μ.-Θ. πραγματοποιείται μόνο για νόμιμους σκοπούς και με νόμιμο τρόπο, σύμφωνα με την κείμενη νομοθεσία.
- Η χρήση των πληροφοριακών συστημάτων και του δικτύου πρέπει να διασφαλίζει την εύρυθμη λειτουργία τους αποφεύγοντας την αναίτια σπατάλη πόρων.
- Η χρήση του διαδικτύου που παρέχεται από την Α.Δ.Μ.-Θ. γίνεται με τρόπο που δεν αντιβαίνει στον υπηρεσιακό ρόλο των χρηστών και δεν διακινδυνεύει την μείωση του κύρους της Υπηρεσίας.
- Οι πληροφορίες που αποκομίζουν οι χρήστες χρησιμοποιούνται μόνο για υπηρεσιακούς σκοπούς. Αν χρειάζεται να μεταδοθούν, μεταδίδονται μόνο σε εξουσιοδοτημένους χρήστες και με ασφαλείς τρόπους.
- Οι χρήστες πρέπει να χειρίζονται και να χρησιμοποιούν τον κάθε είδους εξοπλισμό συστημάτων ή δικτύου με τρόπο που δεν θα προκαλεί φθορές, βλάβες ή και απώλειά του.
- Οι χρήστες πρέπει να αναφέρουν οποιαδήποτε περίπτωση δυσλειτουργίας των συστημάτων που χρησιμοποιούν, αμέσως μόλις κάτι τέτοιο περιέλθει στην αντίληψή τους.

3. Ορθή χρήση των πληροφοριακών συστημάτων της Α.Δ.Μ.-Θ.

3.1 Εμπιστευτικότητα και συμμόρφωση με την προστασία προσωπικών δεδομένων

Οι χρήστες έχουν την ευθύνη να συμβάλλουν στην ασφάλεια των πληροφοριακών συστημάτων της Α.Δ.Μ.-Θ.. Για να το επιτύχουν αυτό, πρέπει :

1. Να τηρούν την αρχή της εμπιστευτικότητας των πληροφοριών που χειρίζονται κατά την άσκηση των καθηκόντων τους. Αποτελεί καλή πρακτική να χειρίζονται ως εμπιστευτικές όλες τις πληροφορίες, συμπεριλαμβανομένων των δεδομένων προσωπικού χαρακτήρα, που περιλαμβάνονται στα έγγραφα τα οποία παραλαμβάνονται ή διακινούνται από αυτούς σε έντυπη ή ηλεκτρονική μορφή. Όταν απαιτείται, πρέπει να συμβουλεύονται τον Υπεύθυνο Προστασίας Δεδομένων (DPO, dpo@m-t.gov.gr).
2. Ιδιαίτερη προσοχή πρέπει να δίνεται στον χειρισμό θεμάτων που χαρακτηρίζονται απόρρητα ή εμπιστευτικά από τις κείμενες διατάξεις ή όταν αυτό επιβάλλεται από την κοινή πείρα και λογική, για γεγονότα ή πληροφορίες των οποίων οι χρήστες λαμβάνουν γνώση ή

επεξεργάζονται κατά την εκτέλεση των καθηκόντων τους. Δεν θα χρησιμοποιούν αυτές τις πληροφορίες για προσωπικό τους όφελος.

3. Να μην αποκαλύπτουν πληροφορίες ή μέρος αυτών παρά μόνον στο ενδιαφερόμενο τρίτο μέρος το οποίο συναλλάσσεται με την Υπηρεσία τους και στους αρμόδιους υπαλλήλους του Τμήματός τους, σύμφωνα με τις ισχύουσες αναθέσεις καθηκόντων από την Διοίκηση.
4. Οι χρήστες πρέπει να έχουν δικαίωμα πρόσβασης / επεξεργασίας μόνο των πληροφοριών που είναι απαραίτητες για την εκτέλεση των καθηκόντων τους.
5. Έχουν την ευθύνη να διασφαλίσουν ότι όλο το υπηρεσιακό υλικό που τηρούν σε ηλεκτρονική μορφή είναι αποθηκευμένο σε οργανωμένους και ταξινομημένους ηλεκτρονικούς φακέλους και είναι εύκολα ανιχνεύσιμο και προσπελάσιμο από τους ίδιους όταν ζητηθεί.
6. Το υπηρεσιακό υλικό σε έντυπη ή ηλεκτρονική μορφή ανήκει στο Δημόσιο και οφείλουν να το παραδώσουν ακέραιο και εξ ολοκλήρου σε κάθε περίπτωση αποχώρησής τους (μόνιμης ή προσωρινής).
7. Η Δ/νση Πληροφορικής & Επικοινωνιών διατηρεί το δικαίωμα να καταγράφει και να τηρεί οποιαδήποτε ενέργεια (όπως καταχώρηση, μεταβολή, διαγραφή, εμφάνιση, εκτύπωση στοιχείων κ.τ.λ.) που πραγματοποιείται στα πληροφοριακά συστήματα της Α.Δ.Μ.-Θ. Οι ενέργειες αυτές μπορούν να αποδοθούν στο άτομο που τις εκτέλεσε.
8. Εάν περιέλθει στην κατοχή κάποιου χρήστη πληροφοριακό σύστημα που περιέχει προσβάσιμα αρχεία τρίτου προσώπου (π.χ. χρήση Η/Υ υπαλλήλου που συνταξιοδοτήθηκε με προσωπικά και υπηρεσιακά δεδομένα στα οποία δεν χρειάζεται να έχει πρόσβαση) οφείλει να ενημερώσει αρμοδίως τον Προϊστάμενό του για το γεγονός.
9. Για τον διαμοιρασμό αρχείων με προσωπικά ή υπηρεσιακά δεδομένα προτείνεται να χρησιμοποιείται η δυνατότητα κοινοποίησης μέσω του Onedrive, του Microsoft Teams και του Microsoft SharePoint.
10. Στους χρήστες που λόγω καθηκόντων έχουν λογαριασμό αυξημένων προνομίων (privileged account) προτείνεται να χορηγείται δεύτερος λογαριασμός απλού χρήστη (non-privileged account) για την εκτέλεση μη διαχειριστικών εργασιών καθημερινής ρουτίνας.
11. Η Δ/νση Πληροφορικής & Επικοινωνιών διατηρεί το δικαίωμα να ζητεί από τους χρήστες να δημιουργηθούν περισσότεροι του ενός λογαριασμοί ανάλογα με τις υπηρεσιακές ανάγκες.
12. Όταν κρίνεται απαραίτητο, μπορεί να ζητηθεί από τους χρήστες η χρήση ταυτοποίησης δύο παραγόντων (2 factor authentication) για τη διασφάλιση μεγαλύτερου επιπέδου ασφάλειας.

3.2 . Λογισμικό

1. Να χρησιμοποιείται μόνο κατάλληλα αδειοδοτημένο λογισμικό και εν γένει να τηρούνται οι διατάξεις που αφορούν στον σεβασμό των δικαιωμάτων πνευματικής ιδιοκτησίας.
2. Η Διεύθυνση Πληροφορικής & Επικοινωνιών έχει δημιουργήσει μια λίστα εγκεκριμένων λογισμικών (software repository, whitelisting) που μπορούν οι χρήστες να χρησιμοποιούν για τις υπηρεσιακές ανάγκες τους. Έχει αφαιρεθεί από τους χρήστες η δυνατότητα εγκατάστασης νέου λογισμικού. Συνεπώς για την εγκατάσταση νέου λογισμικού στους Η/Υ της Υπηρεσίας πρέπει να

ζητείται η συνδρομή της Δ/νσης Πληροφορικής & Επικοινωνιών.

3. Πρέπει να ενημερώνονται τακτικά (στις τελευταίες εκδόσεις) τα λογισμικά που χρησιμοποιούνται (π.χ. λογισμικά εφαρμογών γραφείου, τηλεδιασκέψεων, antivirus, αναγνώστες pdf, web browsers και browser plugins κτλ), λαμβάνοντας υπόψη ότι πολλές από τις ενημερώσεις διορθώνουν κενά ασφάλειας που έχουν εντοπιστεί.
4. Η Δ/νση Πληροφορικής & Επικοινωνιών έχει εγκαταστήσει έναν update server για τη διευκόλυνση της εγκατάστασης των ενημερώσεων των λογισμικών με την ελάχιστη δυνατή χρήση πόρων. Με τη βοήθεια των υπηρεσιών καταλόγου της Microsoft (Active Directory) έχει ενεργοποιηθεί σε όλους τους χρήστες η αυτόματη εγκατάσταση των ενημερώσεων των λειτουργικών συστημάτων (Windows). Σε περίπτωση που διαπιστωθεί ότι δεν είναι ενεργοποιημένη σε κάποιο χρήστη, πρέπει να ζητείται άμεσα η συνδρομή της Δ/νσης Πληροφορικής & Επικοινωνιών.

3.3. Διαχείριση Κωδικών Πρόσβασης

1. Όλοι οι υπάλληλοι του φορέα, εκτός από ορισμένους υπαλλήλους της Δ/νσης Πληροφορικής & Επικοινωνιών, έχουν δικαιώματα απλού χρήστη. Εφόσον για τις υπηρεσιακές τους ανάγκες πρέπει κάποιος υπάλληλος να αποκτήσει αυξημένα δικαιώματα, μπορεί να επικοινωνήσει με τη Δ/νση Πληροφορικής & Επικοινωνιών για την παροχή προσωρινού κωδικού τοπικού διαχειριστή (μέσω του MSLAPS), για την εκτέλεση των απαιτούμενων ενεργειών.
2. Οι χρήστες για την πρόσβαση στον υπηρεσιακό προσωπικό Η/Υ τους θα πρέπει να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης (passwords). Για την επίτευξη του επιθυμητού επιπέδου ασφάλειας προτείνεται οι κωδικοί να έχουν μήκος 12 χαρακτήρες και να περιλαμβάνουν τουλάχιστον ένα μικρό και ένα κεφαλαίο γράμμα, ένα σύμβολο και έναν αριθμό.
3. Οι κωδικοί πρόσβασης δεν πρέπει να περιέχουν ονόματα ή κοινές λέξεις που υπάρχουν σε λεξικά.
4. Οι κωδικοί πρόσβασης είναι αυστηρά προσωπικοί και χαρακτηρίζονται ως εμπιστευτική πληροφορία.
5. Ο κωδικός πρόσβασης πρέπει να είναι διαφορετικός για κάθε υπηρεσιακό ή προσωπικό λογαριασμό που διαθέτουν οι χρήστες.
6. Οι κωδικοί πρόσβασης πρέπει να αλλάζουν τακτικά. Η υπάρχουσα ρύθμισή μας καθιστά υποχρεωτική την αλλάγή τους κάθε 6 μήνες το ελάχιστο.
7. Δεν πρέπει να χρησιμοποιείται ο ίδιος ή παραπλήσιος (προσαρμοσμένος με κάποια επουσιώδη τροποποίηση) κωδικός πρόσβασης για συστήματα που ανήκουν σε εξωτερικά δίκτυα ή υπηρεσίες του διαδικτύου (π.χ. πρόγραμμα «ΔΙΑΥΓΕΙΑ», e-procurement.gov.gr, opendata.gov.gr κ.τ.λ).
8. Οι κωδικοί πρόσβασης δεν πρέπει ποτέ να είναι καταγεγραμμένοι ή αποθηκευμένοι σε μέρη με εύκολη πρόσβαση (π.χ. σε ένα κομμάτι χαρτί εκτεθειμένο πάνω στο πληκτρολόγιο ή σε κάποιο

συρτάρι του γραφείου ή στο ημερολόγιο ή ατζέντα που πιθανόν χρησιμοποιεί ο υπάλληλος) ή σε ψηφιακά αρχεία εύκολα προσβάσιμα.

9. Οι κωδικοί πρόσβασης δεν πρέπει να κοινοποιούνται με κανέναν τρόπο σε οποιονδήποτε τρίτο.
10. Για την αποτελεσματικότερη διαχείριση των κωδικών πρόσβασης, εφόσον και όπου είναι εφικτό, προτείνεται να χρησιμοποιούνται εφαρμογές διαχείρισης κωδικών πρόσβασης με δυνατότητα κρυπτογράφησης.
11. Να μην αποθηκεύονται οι κωδικοί πρόσβασης στους browsers.
12. Οι χρήστες πρέπει να ειδοποιούν άμεσα τον Προϊστάμενο της οργανικής μονάδας που υπηρετούν για τυχόν διαρροή κωδικών, δικών τους ή τρίτων, που έχει υποπέσει στην αντίληψή τους.
13. Η επιφάνεια εργασίας του Η/Υ πρέπει να κλειδώνεται με τον προσωπικό κωδικό όταν ο χρήστης απουσιάζει από το γραφείο του. Η Διεύθυνση Πληροφορικής & Επικοινωνιών διασφαλίζει ότι ενεργοποιείται το κλείδωμα της οθόνης μετά από μέγιστο χρονικό διάστημα 15 λεπτών αδράνειας του χρήστη, με σκοπό την αποφυγή μη εξουσιοδοτημένης πρόσβασης. Προκειμένου να ξεκλειδωθεί η οθόνη, απαιτείται η εκ νέου αυθεντικοποίηση του χρήστη.
14. Εάν κάποιος χρήστης διαπιστώσει ότι ο λογαριασμός του παρέχει δυνατότητες πρόσβασης /επεξεργασίας σε επιπλέον πληροφορίες από αυτές που απαιτούνται για την εκτέλεση των καθηκόντων του, οφείλει αμελλητί να ενημερώσει τον Προϊστάμενό του, ο οποίος πρέπει να επικοινωνήσει άμεσα με την Δ/νση Πληροφορικής & Επικοινωνιών.
15. Ο Προϊστάμενος της Υπηρεσίας οφείλει να ενημερώνει άμεσα και εγγράφως τη Δ/νση Πληροφορικής & Επικοινωνιών σχετικά με την αποχώρηση υπαλλήλου από την Υπηρεσία, έτσι ώστε να γίνεται αφαίρεση των δικαιωμάτων πρόσβασης του υπαλλήλου στις εφαρμογές και τα υπηρεσιακά αρχεία.

3.4 . Ορθή χρήση των Πληροφοριακών Συστημάτων

1. Τα Πληροφοριακά Συστήματα που παραχωρούνται στους χρήστες είναι περιουσιακά στοιχεία της Α.Δ.Μ.-Θ. και ως εκ τούτου η χρήση τους πρέπει να συμμορφώνεται με την παρούσα πολιτική.
2. Δεν επιτρέπεται η χρήση του εξοπλισμού της Υπηρεσίας από μη εξουσιοδοτημένα πρόσωπα (επισκέπτες κ.ά).
3. Οι χρήστες δεν πρέπει να εγκαθιστούν/συνδέουν εξοπλισμό (Η/Υ, ασύρματα σημεία πρόσβασης κ.α.) στα δίκτυα της Α.Δ.Μ.-Θ. .
4. Οι χρήστες δεν πρέπει να χρησιμοποιούν ασύρματους προσαρμογείς (usb wifi adaptors) για σύνδεση του Η/Υ της Υπηρεσίας σε άλλο δίκτυο (π.χ. δίκτυο παρόχου τηλεπικοινωνιακών υπηρεσιών).
5. Απαγορεύεται η μη εξουσιοδοτημένη πρόσβαση στον προσωπικό εξοπλισμό, λογαριασμό ή ιδιωτική επικοινωνία των άλλων χρηστών. Σε περίπτωση που οποιοσδήποτε χρήστης αποκτήσει ακούσια τέτοια πρόσβαση, οφείλει να την τερματίσει αμέσως και να προβεί σε άμεση ειδοποίηση του επηρεαζόμενου προσώπου για το συμβάν **.**
6. Εφόσον χρησιμοποιείται κινητό τηλέφωνο για πρόσβαση σε εφαρμογές ή υπηρεσίες της Α.Δ.Μ.-

Θ., να μην γίνεται σύνδεση σε κοινόχρηστο wifi δίκτυο και να είναι απενεργοποιημένο το Bluetooth.

7. Η χρήση φορητών μέσων αποθήκευσης (USB, εξωτερικούς σκληρούς δίσκους, CD, DVD) που είναι άγνωστης προέλευσης απαγορεύεται.
8. Εφόσον για τις υπηρεσιακές ανάγκες είναι απαραίτητο να γίνει χρήση φορητού μέσου αποθήκευσης, πρέπει να διασφαλίζεται ότι διενεργείται αυτόματα σάρωση για κακόβουλο λογισμικό σε φορητά μέσα αποθήκευσης, όταν αυτό συνδέεται σε συσκευές που έχουν πρόσβαση στους δίκτυο της Α.Δ.Μ.-Θ..
9. Πρέπει να διασφαλίζεται ότι δεν θα αποκτήσει πρόσβαση σε φορητό μέσο αποθήκευσης μη εξουσιοδοτημένος χρήστης.
10. Τα φορητά μέσα αποθήκευσης δεν πρέπει να συνδέονται με συστήματα που δεν ανήκουν στην Α.Δ.Μ.-Θ., εκτός αν μπορεί να διασφαλιστεί ότι δεν θα μολυνθούν από κακόβουλο λογισμικό **.**
11. Τα υπηρεσιακά ψηφιακά αρχεία πρέπει να αποθηκεύονται στα κοινόχρηστα μέσα αποθήκευσης (βιβλιοθήκες του Microsoft Teams και SharePoint που έχουμε δημιουργήσει για όλες τις οργανικές μας μονάδες). Για την τήρηση ατομικών αντιγράφων ασφαλείας προτείνεται να χρησιμοποιείται ο προσωπικός χώρος που ο κάθε χρήστης έχει στο Onedrive. Τα δεδομένα είναι κρυπτογραφημένα στους διακομιστές της Microsoft (σε ανάπαυση) και κατά την ανταλλαγή/μετάδοσή τους μέσω του διαδικτύου. Εφόσον οι χρήστες το επιθυμούν, για μεγαλύτερη ασφάλεια, μπορούν να κάνουν τακτικά λήψη των αρχείων στον προσωπικό υπολογιστή που τους παρέχεται από την Α.Δ.Μ.-Θ..
12. Δεν πρέπει να είναι ενεργοποιημένος ο αυτόματος συγχρονισμός των αρχείων που υπάρχουν στον προσωπικό υπολογιστή των χρηστών με το OneDrive, καθώς μπορεί να συμβάλλει στη διασπορά ιών και κακόβουλου λογισμικού.
13. Κατά την σύνδεση με τους κοινόχρηστους φακέλους της Υπηρεσίας - στους οποίους παρέχεται πρόσβαση με άδεια της Υπηρεσίας – πρέπει να λαμβάνεται υπόψη ότι οποιαδήποτε ενέργεια (π.χ. διαγραφή αρχείου) επηρεάζει τη λειτουργία όλων των υπαλλήλων που έχουν κοινή πρόσβαση στον κοινόχρηστο φάκελο.
14. Δεν επιτρέπεται η αποθήκευση μη υπηρεσιακών αρχείων στο δίκτυο και τους πόρους της Α.Δ.Μ.-Θ..
15. Όλοι οι υπολογιστές ή άλλες συσκευές που χρησιμοποιούνται για απομακρυσμένη πρόσβαση στο δίκτυο της Α.Δ.Μ.-Θ. πρέπει να ικανοποιούν τις απαιτήσεις της παρούσας πολιτικής. Επίσης, οι χρήστες οφείλουν να εξασφαλίσουν ότι ο εξοπλισμός που χρησιμοποιούν πληροί κάποιες βασικές προδιαγραφές ασφάλειας (π.χ. να εγκαταστήσουν λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό και να χρησιμοποιούν τείχος προστασίας).
16. Για την εκτέλεση απομακρυσμένης εργασίας που αφορά σε εφαρμογές γραφείου από χώρους εκτός των εγκαταστάσεων της Α.Δ.Μ.-Θ. πρέπει να χρησιμοποιούνται το Microsoft Teams, τα Office 365 και το OneDrive του κάθε χρήστη. Δεν υπάρχει πλέον κανένας λόγος να χρησιμοποιείται η απομακρυσμένη πρόσβαση για το σκοπό αυτό.
17. Όταν η απομακρυσμένη πρόσβαση απαιτείται για την εκτέλεση εργασιών εκτός της χρήσης του Office 365, πρέπει να χρησιμοποιείται VPN.
18. Κατά την αντικατάσταση ή παράδοση Η/Υ από μία Υπηρεσία σε άλλη, απαιτείται η παραλαβή

όλων των υπηρεσιακών δεδομένων από την παραδίδουσα Υπηρεσία και, εν συνεχεία, η διαγραφή όλων των δεδομένων από τον Η/Υ με ευθύνη της Δ/νσης Πληροφορικής & Επικοινωνιών.

19. Οι αίθουσες των servers πρέπει να είναι κλειδωμένες. Μόνο προσωπικό εξουσιοδοτημένο από την Δ/νση Πληροφορικής & Επικοινωνιών θα πρέπει να μπορεί να έχει πρόσβαση σε αυτές.
20. Πρέπει να απενεργοποιούνται οι συσκευές κατά την αποχώρηση από τον χώρο εργασίας μετά τη λήξη του ωραρίου.

3.5 . Ορθή χρήση του διαδικτύου και του ηλεκτρονικού ταχυδρομείου

1. Η χρήση του διαδικτύου και του υπηρεσιακού ηλεκτρονικού ταχυδρομείου (email) πρέπει να γίνεται με τρόπο που δεν αντιβαίνει στον υπηρεσιακό ρόλο του χρήστη και δεν προσβάλλει το κύρος του Δημοσίου και της Α.Δ.Μ.-Θ.
2. Απαγορεύεται αυστηρά η αποστολή, προώθηση και αποθήκευση πληροφοριών και αρχείων που σχετίζονται με παράνομες ή ανάρμοστες δραστηριότητες.
3. Οι χρήστες δεν πρέπει να αποστέλλουν ή να προωθούν μηνύματα ηλεκτρονικού ταχυδρομείου ή δημοσιεύσεις που προσβάλλουν, συκοφαντούν, δυσφημούν, απειλούν, ενοχλούν ή κακοποιούν με οποιονδήποτε τρόπο άτομα, νομικά πρόσωπα, χώρες, έθνη, εθνικότητες, σεξουαλικούς προσανατολισμούς, θρησκείες, πολιτικές πεποιθήσεις και σωματικές αναπηρίες, καθώς και μηνύματα που ενδέχεται να έχουν νομικές ή άλλες συνέπειες για την Α.Δ.Μ.-Θ.
4. Απαγορεύεται η διακίνηση μηνυμάτων με παράνομο ή με κακόβουλο/ιομορφικό λογισμικό.
5. Οι χρήστες θα πρέπει να γνωρίζουν ότι υπάρχει κίνδυνος εισαγωγής κακόβουλου λογισμικού κατά την επίσκεψη τους σε διαδικτυακές ιστοσελίδες. Εάν κάποιος χρήστης ανακαλύψει ότι επισκέφθηκε κάποια ιστοσελίδα που φαίνεται να ενεργεί ασυνήθιστα, θα πρέπει να αποσυνδεθεί αμέσως από αυτήν και να αναφέρει το συμβάν στην Διεύθυνση Πληροφορικής & Επικοινωνιών.
6. Δεν πρέπει να χρησιμοποιείται το υπηρεσιακό email για την αποστολή μη υπηρεσιακών δεδομένων/αρχείων, που εμπίπτουν στην ιδιωτική ζωή ή αφορούν άσκηση ιδιωτικού έργου με αμοιβή (ή μη) καθόσον αυτό (το έργο) αφορά εργασία που δεν σχετίζεται με τα υπηρεσιακά καθήκοντα.
7. Δεν πρέπει να χρησιμοποιούνται λογαριασμοί ηλεκτρονικού ταχυδρομείου τρίτων παρόχων για υπηρεσιακούς σκοπούς.
8. Απαγορεύεται η χρήση των πόρων της Α.Δ.Μ.-Θ. για προσωπικούς σκοπούς.
9. Όταν ένα μήνυμα ηλεκτρονικού ταχυδρομείου έχει πολλούς αποδέκτες ή αποστέλλεται σε λίστα αποδεκτών, πρέπει να χρησιμοποιείται η κρυφή/ιδιαίτερη κοινοποίηση **.**
10. Πρέπει να αποφεύγεται η διακίνηση εμπιστευτικών/απόρρητων πληροφοριών και προσωπικών δεδομένων πολιτών ή υπαλλήλων μέσω ηλεκτρονικού ταχυδρομείου. Εφόσον αυτό είναι υποχρεωτικό για λόγους υπηρεσιακούς, θα πρέπει να λαμβάνονται μέτρα που καθιστούν ασφαλή τη μετάδοση της πληροφορίας (π.χ. κρυπτογράφηση) σε συνεννόηση με τον

υπηρεσιακό αποδέκτη και τη συνδρομή της Δ/νσης Πληροφορικής και Επικοινωνιών.

11. Οι χρήστες δεν πρέπει να αποστέλλουν σε άλλους χρήστες ανεπιθύμητα ηλεκτρονικά μηνύματα (unsolicited mails ή junk mails) ή άλλου διαφημιστικού ή προωθητικού περιεχομένου (spams).
12. Κάθε email από άγνωστο παραλήπτη πρέπει να αντιμετωπίζεται με ιδιαίτερη προσοχή. Ο πρώτος έλεγχος που θα διενεργείται είναι αν η διεύθυνση του email έχει σχέση με την ιδιότητα που αναφέρεται στο θέμα ή στο σώμα του email. Αν το email υποτίθεται ότι είναι από αποστολέα με συγκεκριμένη ιδιότητα και η διεύθυνση του email είναι εντελώς διαφορετική ή δεν συνδέεται με την ιδιότητα του αποστολέα, πρέπει να θεωρηθεί spam (π.χ. ένας υπάλληλος της Α.Δ.Μ.-Θ. θα έχει διεύθυνση email της μορφής username@m-t.gov.gr ή της Εθνικής Αρχής Διαφάνειας θα έχει τη μορφή username@aead.gr).
13. Πρέπει να ελέγχεται αν το email είναι υπογεγραμμένο. Η υπογραφή στο email θα πρέπει να περιλαμβάνει το ονοματεπώνυμο του αποστολέα, την ιδιότητά του, τον φορέα ή την εταιρία στην οποία εργάζεται και τους τρόπους επικοινωνίας (τηλέφωνο, διεύθυνση ηλεκτρονικού ταχυδρομείου κτλ).
14. Εφόσον δεν ταυτοποιηθεί ο αποστολέας και δεν προηγηθεί επικοινωνία με αυτόν, δεν θα ανοίγονται τυχόν συνημμένα αρχεία ή σύνδεσμοι ηλεκτρονικών διευθύνσεων (links). Αν εκ παραδρομής ο χρήστης προβεί σε σχετική ενέργεια, πρέπει να ενημερώνεται άμεσα η Δ/νση Πληροφορικής & Επικοινωνιών.
15. Τα προσωπικά και υπηρεσιακά στοιχεία των χρηστών δεν θα καταχωρούνται σε τρίτους ιστότοπους πέρα από αυτούς που σχετίζονται με την ανάθεση των καθηκόντων του χρήστη.
16. Τα προγράμματα πλοήγησης και ηλεκτρονικού ταχυδρομείου πρέπει να ενημερώνονται τακτικά. Εφόσον διαπιστωθεί ότι δεν είναι ενημερωμένα, πρέπει να ζητείται η συνδρομή της Δ/νσης Πληροφορικής & Επικοινωνιών **.**
17. Η λήψη, αναπαραγωγή ή αναδιανομή υλικού που αποτελεί πνευματική ιδιοκτησία, όπως μουσική, ταινίες, εικόνες ή λογισμικό, ενδέχεται να συνιστά παραβίαση των νόμων ή των κανονισμών σε πολλές χώρες και να επισύρει πειθαρχικές ή ποινικές κυρώσεις.

3.6 Χρήση τηλεφωνικού εξοπλισμού

1. Στους χρήστες διατίθεται τηλεφωνικός εξοπλισμός της Α.Δ.Μ.-Θ. ως μέσο διευκόλυνσης της εκτέλεσης των υπηρεσιακών τους καθηκόντων.
2. Ο τηλεφωνικός εξοπλισμός είναι περιουσιακό στοιχείο της Α.Δ.Μ.-Θ. και ως εκ τούτου η χρήση του πρέπει να συμμορφώνεται με την παρούσα πολιτική.
3. Ιδιαίτερη προσοχή πρέπει να δοθεί σε πιθανές επιθέσης Κοινωνικής Μηχανικής μέσω τηλεφωνικών κλήσεων. Πρόκειται για προσπάθεια προφορικής χειραγώγησης ατόμων με σκοπό την απόσπαση πληροφοριών που μπορεί αρχικά να φαίνονται ασήμαντες στον χρήστη. Οι χρήστες πρέπει να διασφαλίζουν πάντα ότι γνωρίζουν ποιος τους ζητά στοιχεία και ότι είναι εξουσιοδοτημένος να έχει πρόσβαση στην πληροφορία που ζητά και να μην παρέχουν πληροφορίες που δεν είναι σίγουροι ότι αφορούν τον συνομιλητή τους.
4. Οι χρήστες δεν πρέπει να απαντούν σε ερωτήματα σχετικά με προσωπικά δεδομένα άλλων υπαλλήλων της Α.Δ.Μ.-Θ. ούτε να κοινοποιούν στοιχεία αυθεντικοποίησης μέσω τηλεφώνου σε

τρίτους.

5. Οι χρήστες δεν πρέπει να χρησιμοποιούν τον τηλεφωνικό εξοπλισμό για καταχρηστικές, βίαιες, συκοφαντικές, απειλητικές ή παρενοχλητικές κλήσεις.

Η παρούσα πολιτική μπορεί να τροποποιηθεί σύμφωνα με τις εκάστοτε τρέχουσες ανάγκες της Α.Δ.Μ.-Θ., προκειμένου να προσαρμόζεται σε καταστάσεις που μπορεί να προκύψουν ή κινδύνους που μπορεί να εντοπιστούν.

Σας εφιστούμε την προσοχή καθώς, σύμφωνα με τις διατάξεις της νομοθεσίας που αναφέρεται στην παρούσα πολιτική, οποιαδήποτε ενέργεια μπορεί να προκαλέσει φθορά λόγω ασυνήθιστης χρήστης ή εγκατάλειψη ή παράνομη χρήση των πληροφοριακών συστημάτων ενός δημόσιου φορέα επισύρει πειθαρχικές αλλά και εν δυνάμει ποινικές κυρώσεις.

Καλούνται όλοι οι χρήστες των πόρων της Α.Δ.Μ.-.Θ. να συμβάλλουν ενεργά, ανάλογα με το ρόλο που ανατίθεται στον καθένα, για την επιτυχή εφαρμογή της παρούσας πολιτικής με πνεύμα συνεργασίας και συναδερφικότητας. Οποιοσδήποτε χρήστης διαπιστώσει ότι υπάρχει κάποια παράλειψη ή κενό στην παρούσα ή για την υποβολή οποιασδήποτε πρότασης βελτίωσης μπορεί να απευθύνεται στη Διεύθυνση Πληροφορικής & Επικοινωνιών της Α.Δ.Μ.-Θ.

Ο Γραμματέας
Αποκεντρωμένης Διοίκησης Μακεδονίας-Θράκης

Δρ. Ιωάννης Σάββας