ΚΑΝΟΝΙΣΜΟΣ ΑΣΦΑΛΕΙΑΣ
ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

1. ΣΚΟΠΟΣ ΚΑΙ ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Ο παρόν Κανονισμός αποσκοπεί στην καθιέρωση κανόνων ασφαλούς, υπεύθυνης και αποτελεσματικής χρήσης των πληροφοριακών συστημάτων και των υποδομών Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) του Δήμου Περιστερίου.

Αφορά όλους όσους έχουν εξουσιοδοτημένη πρόσβαση στα συστήματα του Δήμου (εργαζομένους, αιρετούς, εξωτερικούς συνεργάτες, συμβασιούχους) και τους εργαζόμενους/διαχειριστές του τμήματος Πληροφορικής (IT).

2. ΓΕΝΙΚΕΣ ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ (ισχύουν για όλους τους ΧΡΗΣΤΕΣ)

1. Κάθε χρήστης οφείλει να κάνει υπεύθυνη χρήση του υπολογιστή, των δικτυακών πόρων, της πρόσβασης στο internet και της ηλεκτρονικής του διεύθυνσης.

2. Κάθε χρήστης οφείλει να χρησιμοποιεί ισχυρό κωδικό πρόσβασης στον προσωπικό του λογαριασμό πρόσβασης στα Windows και στο δίκτυο. Ο κωδικός πρέπει να αλλάζει σύμφωνα με τις οδηγίες του IT και όποτε επιθυμεί ο χρήστης.
   Video οδηγιών αλλαγής password **εδώ…**

3. Κάθε χρήστης οφείλει να χρησιμοποιεί ισχυρούς κωδικούς πρόσβασης σε λογισμικά και πλατφόρμες, τους οποίους εάν αποθηκεύει, αυτό να γίνεται σε κλειδωμένο ηλεκτρονικό αρχείο.
   Υπόδειγμα αρχείου **εδώ…**
   Video οδηγιών κλειδώματος αρχείου **εδώ…**

4. Κάθε χρήστης οφείλει να ελέγχει τον αποστολέα στα εισερχόμενα email και σε περίπτωση που είναι άγνωστος ή παραπλανητικός, το email να διαγράφεται χωρίς να ανοιχθεί.
   Video οδηγιών αναγνώρισης παραπλανητικού email **εδώ…**

5. Κάθε χρήστης οφείλει να κλείνει τον υπολογιστή του ή να αφήνει την οθόνη σε κατάσταση κλειδώματος όταν απομακρύνεται από την θέση του.

6. Δεν επιτρέπεται η κοινή χρήση λογαριασμών πρόσβασης μεταξύ χρηστών.

7. Δεν επιτρέπεται η εγκατάσταση λογισμικού χωρίς έγκριση από το IT.

8. Δεν επιτρέπεται η σύνδεση USB sticks και εξωτερικών δίσκων χωρίς έλεγχο από το IT.

9. Δεν επιτρέπεται ή σύνδεση φορητών Η/Υ (laptops) στο δίκτυο χωρίς έλεγχο από το IT.

10. Δεν επιτρέπεται η αποθήκευση προσωπικών αρχείων στους δικτυακούς καταλόγους.

11. Κάθε χρήστης είναι υπεύθυνος για την λήψη αντιγράφων ασφαλείας αρχείων που δεν είναι αποθηκευμένοι σε δικτυακούς καταλόγους.

12. Κάθε χρήστης ακολουθεί τις οδηγίες διαχείρισης και κρυπτογράφησης προσωπικών δεδομένων όπως ορίζονται από τον Υπεύθυνο Προσωπικών Δεδομένων του Δήμου (DPO).

13. Κάθε χρήστης οφείλει να ενημερώνεται για ζητήματα ασφαλούς χρήσης Η/Υ και διαδικτύου και να παρακολουθεί σχετικά εκπαιδευτικά σεμινάρια.

14. Οποιοδήποτε περιστατικό ασφάλειας πρέπει να αναφέρεται άμεσα στο ΙΤ.

3. ΚΑΘΗΚΟΝΤΑ ΠΡΟΙΣΤΑΜΕΝΩΝ ΟΡΓΑΝΙΚΩΝ ΜΟΝΑΔΩΝ

1. Κάθε προϊστάμενος οργανικής μονάδας οφείλει να διατηρεί ενημερωμένο εσωτερικό αρχείο/μητρώο υπηρετούντων υπαλλήλων/χρηστών με τα username και τα δικαιώματα χρήσης δικτυακών πόρων και λογαριασμών των χρηστών/υπαλλήλων της οργανικής του μονάδας.
   Υπόδειγμα αρχείου μητρώου **εδώ…**

2. Κάθε προϊστάμενος οργανικής μονάδας οφείλει να χρησιμοποιεί την φόρμα «Αιτήματα δικτυακής πρόσβασης» για κάθε επιθυμητή αλλαγή σε δικαιώματα πρόσβασης χρηστών/υπαλλήλων της οργανικής του μονάδας όπως:
   - Νέος υπάλληλος.
   - Αποχώρηση Υπαλλήλου.
   - Απόδοση ή αλλαγές δικαιωμάτων πρόσβασης σε εφαρμογές η δικτυακούς καταλόγους.
   - Επέκταση ή αλλαγές στα ημερήσια χρονικά δικαιώματα πρόσβασης.
   - Απόδοση προσωπικής διεύθυνσης email κ.λ.π.

   Φόρμα «Αιτήματα δικτυακής πρόσβασης» **εδώ…**

3. Κάθε προϊστάμενος οργανικής μονάδας οφείλει να γνωρίζει και να επιβλέπει την ορθή χρήση των δικτυακών καταλόγων που χρησιμοποιεί η υπηρεσία του. Οφείλει σε συνεργασία με το ΙΤ να επιβλέπει τα δικαιώματα χρήσης των δικτυακών καταλόγων και σε κάθε περίπτωση είναι υπεύθυνος για τα δεδομένα τα οποία αποθηκεύει η υπηρεσία του.

4. Κάθε προϊστάμενος οργανικής μονάδας οφείλει να παρακινεί το προσωπικό της υπηρεσίας του να ενημερώνεται για ζητήματα ασφαλούς χρήσης Η/Υ και διαδικτύου και να παρακολουθεί σχετικά εκπαιδευτικά σεμινάρια.

Κείμενα οδηγιών, υποδείγματα εγγράφων, εκπαιδευτικά video, κατάλογος χρήσιμων ιστοσελίδων, Νομοθεσία, βοηθητικά εργαλεία κ.λ.π στον ΟΔΗΓΟ ΥΠΑΛΛΗΛΟΥ **εδώ…**
