Δήμος Περιστερίου

ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

ΠΡΟΣΒΑΣΗ

1. Η πρόσβαση στα Windows και στο Δίκτυο του Δήμου γίνεται με το username που έχει ορισθεί από το τμήμα Πληροφορικής του Δήμου (για συντομία: ΤΠ) και με συνθηματικό (password) που ορίζει ο χρήστης.

   Κάθε χρήστης είναι υπεύθυνος για την επιλογή και τη διαφύλαξη ασφαλούς password. Τα passwords δεν πρέπει ποτέ να γράφονται σε χαρτί ούτε να δίνονται σε τρίτους.

   Το password έχει ορισθεί από το ΤΠ να αλλάζει ανά τρεις (3) μήνες. Αλλαγή μπορεί να γίνει και οποιαδήποτε άλλη στιγμή επιθυμεί ο χρήστης και οπωσδήποτε όταν υπάρχουν ενδείξεις παραβίασης. Το password πρέπει να είναι το λιγότερο 6 χαρακτήρες.

   Video οδηγιών αλλαγής password **εδώ**.

2. Το username συνδέεται με συγκεκριμένο χρήστη, συγκεκριμένο υπολογιστή, και συγκεκριμένο ωράριο πρόσβασης. Επίσης συνδέεται με τα ανάλογα της υπαλληλικής θέσης δικαιώματα πρόσβασης σε λογισμικό, δικτυακούς καταλόγους αρχείων και δυνητικά συνδέεται με προσωπική ηλεκτρονική διεύθυνση (e-mail).
   Κάθε αλλαγή στα παραπάνω για οποιονδήποτε χρήστη/υπάλληλο εμπλέκει ζητήματα ασφάλειας και διαχείρισης προσωπικών δεδομένων (Κανονισμός GDPR), και για να υλοποιηθεί χρειάζεται αίτημα (ticket) του άμεσα προϊσταμένου προς το ΤΠ.
   Φόρμα αιτήματος **εδώ**.

ΚΕΝΑ ΑΣΦΑΛΕΙΑΣ / ΟΔΗΓΙΕΣ

3. Σημαντικό κενό ασφαλείας δημιουργείται εάν ο Η/Υ μείνει ανοικτός μετά το πέρας του ωραρίου εργασίας. Σε περίπτωση που ο υπολογιστής χρειάζεται να μείνει ανοικτός αυτό να γίνει σε κατάσταση εισαγωγής password (locked).

4. Σημαντικό κενό ασφαλείας δημιουργείται από Η/Υ που παραμένει σε υπηρεσία χωρίς να έχει ενεργό χρήστη. Σε κάθε περίπτωση συνταξιοδότησης, μετακίνησης, μακροχρόνιας αδείας υπαλλήλου ο άμεσα προϊστάμενος υποχρεούται να ενημερώσει άμεσα το ΤΠ ώστε ή να μετακινηθεί ο Η/Υ ή κατ' ελάχιστον να ακυρωθεί το συγκεκριμένο username του αποχωρήσαντος υπαλλήλου.

5. Σημαντικό κενό ασφαλείας δεδομένων υπάρχει σε δικτυακούς καταλόγους αρχείων που η πρόσβαση είναι ελεύθερη. Είναι επιθυμητό οι υπηρεσίες να φροντίζουν συνεχώς σε συνεργασία με το ΤΠ να ζητούν πρόσβαση στους καταλόγους που διατηρούν στους servers, αποκλειστικά και μόνο στους χρήστες που θα επιλέξουν.
   Φόρμα αιτήματος **εδώ…**

6. Σημαντικό κενό ασφαλείας υπάρχει σε όλα τα συστήματα από τα memory sticks (φλασάκια) που εισάγονται σε διαφορετικούς υπολογιστές και είναι δυνατόν να μεταδώσουν ιούς Η/Υ. Το ΤΠ κάνει ισχυρή σύσταση για την μη χρήση τους, και σε κάθε περίπτωση διατηρεί το δικαίωμα να αποκλείσει μονομερώς την πρόσβαση στις θύρες usb των υπολογιστών.

7. Σημαντικό κενό ασφαλείας υπάρχει σε όλα τα συστήματα από την ηλεκτρονική αλληλογραφία (email). Ισχυρή είναι η σύσταση προς τους χρήστες να μην ανοίγουν email και οπωσδήποτε να μην ανοίγουν συνημμένα αρχεία εφόσον ο αποστολέας είναι άγνωστος.
   Video οδηγιών αναγνώρισης παραπλανητικού email **εδώ…**

8. Σημαντικό κενό ασφαλείας δημιουργείται επίσης εάν για κάποιο λόγο το endpoint antivirus λογισμικό (Kaspersky) δεν είναι ενημερωμένο (updated). Εάν ο χρήστης διαπιστώσει ότι αυτό συμβαίνει θα πρέπει άμεσα να έρθει σε επαφή με τον υπεύθυνο ασφαλείας του ΤΠ.

Υπεύθυνος Ασφαλείας:
Παναγιώτης Σταμάτης
☎ 114
✉ pstamatis@peristeri.gr