ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

# *Οδηγίες για ενσωμάτωση της προστασίας των προσωπικών δεδομένων στις πολιτικές/ διαδικασίες του Bring Your Own Device (BYOD)*

***ΟΔΗΓΙΕΣ**: Το υπόψη κείμενο πρέπει να:*
*Α. Είναι διαθέσιμο στους Επικεφαλής των Διευθύνσεων, Αυτοτελών Τμημάτων και Σχολών*
*Β. Είναι διαθέσιμο στη Διεύθυνση Τεχνικών Υπηρεσιών & Μηχανοργάνωσης*
*Γ. Είναι διαθέσιμο στη ΜΟΔΙΠ*
*Δ. Διατεθεί σε όλους τους εργαζόμενους του Π.Δ.Μ*
*Ε. Είναι διαθέσιμο στο Γραφείο του Υπευθύνου Προστασίας Δεδομένων*
*ΣΤ. Είναι διαθέσιμο σε οποιοδήποτε άλλο Τμήμα κριθεί απαραίτητο από την Υπηρεσία*

## Σκοπός

Σκοπός του παρόντος κειμένου είναι να περιγράφουν οι Οδηγίες για την ενσωμάτωση της προστασίας των προσωπικών δεδομένων στις πολιτικές/ διαδικασίες του Bring Your Own Device (BYOD) από το Π.Δ.Μ..

## Εξαιρέσεις - Πεδίο εφαρμογής

Το αντικείμενο αυτού του εγγράφου περιλαμβάνει τις οδηγίες που ακολουθεί το Π.Δ.Μ. για την ενσωμάτωση της προστασίας των προσωπικών δεδομένων στις πολιτικές / διαδικασίες του Bring Your Own Device (BYOD), σε συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων.
Το κείμενο αποτελεί μέρος της συμμόρφωσης του Π.Δ.Μ. με τον Γ.Κ.Π.Δ.
Αυτό το κείμενο απευθύνεται στο προσωπικό και τους εξωτερικούς συνεργάτες του Π.Δ.Μ.

## Οδηγίες για την ενσωμάτωση της προστασίας των προσωπικών δεδομένων στις πολιτικές/ διαδικασίες του Bring Your Own Device (BYOD)

Με τον όρο Bring Your Own Device εννοείται πρακτική, με βάση την οποία οι υπάλληλοι χρησιμοποιούν, για υπηρεσιακούς λόγους, ιδιόκτητες συσκευές (έξυπνα τηλέφωνα, tablets, φορητούς υπολογιστές και άλλες πλατφόρμες) για πρόσβαση σε υπηρεσιακές εφαρμογές, όπως ηλεκτρονικό ταχυδρομείο και βάσεις δεδομένων, αλλά και για δημιουργία, αποθήκευση και διαχείριση υπηρεσιακών δεδομένων. Το Π.Δ.Μ. κατά κανόνα δεν επιθυμεί οι εργαζόμενοι να χρησιμοποιούν τις προσωπικές τους συσκευές για την εκτέλεση της εργασίας τους, διότι το Π.Δ.Μ. διαθέτει επαρκή εξοπλισμό πληροφορικής για την πρόσβαση σε δεδομένα και πληροφορίες με τη χρήση ιδιόκτητων του πληροφοριακών αγαθών. Αντιλαμβάνεται όμως ότι σε κάποιες ειδικές περιπτώσεις, οι οποίες πρέπει να οριστούν από το Π.Δ.Μ. αποτελούν εξαιρέσεις στον παραπάνω κανόνα η χρήση προσωπικών συσκευών δεν μπορεί να αποφευχθεί. Για αυτές τις περιπτώσεις το Π.Δ.Μ. δηλώνει στους χρήστες τις ακόλουθες υποχρεώσεις :

1. Ο χρήστης μεριμνά για την προστασία της συσκευής του, σε επίπεδο ανίχνευσης virus/malware ή οποιουδήποτε άλλου κακόβουλου κώδικα μέσω εφαρμογής ασφαλείας.
2. Το τοίχος προστασίας της συσκευής πρέπει να είναι ενεργοποιημένο.
3. Η συσκευή πρέπει να αποθηκεύει τα δεδομένα με κρυπτογράφηση.

4. Για τις κινητές έξυπνες συσκευές χειρός ή παλάμης πρέπει να έχει ενεργοποιηθεί εφαρμογή λύσης Anti-Theft ή Remote Wipe, για την προστασία των δεδομένων σε περίπτωση απώλειας/κλοπής εκ μέρους των χρηστών.
5. Ο χρήστης πρέπει να αποφεύγει την αποθήκευση κωδικών πρόσβασης: Η προσωρινή αποθήκευση κωδικών πρόσβασης στις κινητές συσκευές θα πρέπει να αποφεύγεται εάν είναι δυνατόν. Αυτό σημαίνει ότι δεν πρέπει να επιλέγεται το πλαίσιο ελέγχου "Αποθήκευση κωδικού πρόσβασης" σε έναν ιστότοπο ή μια οθόνη εφαρμογής που ζητά τα διαπιστευτήρια.
6. Αν ο χρήστης αποφασίσει να αποθηκεύσει προσωρινά έναν κωδικό πρόσβασης σε μια κινητή συσκευή, πρέπει να βεβαιωθεί ότι προστατεύεται η συσκευή με κωδικό πρόσβασης.
7. Η ενεργοποίηση ενός κωδικού πρόσβασης θα πρέπει επίσης να περιλαμβάνει μια ρύθμιση χρονοκαθυστέρησης για να κλειδώνει η συσκευή (απαιτεί έναν κωδικό πρόσβασης ξανά) μετά από μια παρατεταμένη περίοδο μη δραστηριότητας. Δεκαπέντε λεπτά θεωρείται γενικά μια καλή χρονική περίοδος.
8. Εάν ο χρήστης βρίσκεται σε δημόσιο χώρο αποθαρρύνεται η χρήση δημόσιου κοινόχρηστου Wi-Fi, αλλιώς δημιουργήστε μια συνεδρία VPN.
9. Το Bluetooth πρέπει να είναι ανενεργό όταν δεν χρησιμοποιείται.
10. Αν χαθεί μια συσκευή, ο χρήσης οφείλει να:
    i. Ενημερώσει άμεσα τον άμεσα προϊστάμενο του.
    ii. Αλλάξει οποιονδήποτε κωδικό πρόσβασης έχει στη συσκευή του.

Σε περίπτωση παραβίασης δπχ που οδηγούν την προσωπική σας συσκευή ως πηγή της απειλής το Π.Δ.Μ. δικαιούται να προβεί σε έλεγχο των αποθηκευμένων δεδομένων που βρίσκονται στον υπολογιστή/συσκευή του εργαζομένου, ήτοι στην περίπτωση που η εν λόγω πρόσβαση (επεξεργασία) είναι απολύτως αναγκαία για το σκοπό που επιδιώκει ως υπεύθυνος επεξεργασίας και υπό τον όρο ότι αυτός υπερέχει προφανώς των δικαιωμάτων και συμφερόντων του εργαζομένου, χωρίς να θίγονται οι θεμελιώδεις ελευθερίες αυτού. Ειδικότερα, σκοπός μπορεί να συνιστά από το Π.Δ.Μ. η διασφάλιση της εύρυθμης λειτουργίας του δημόσιου συμφέροντος καθώς και η ανάγκη του να προστατέψει το δημόσιο συμφέρον από σημαντικές απειλές, όπως το να εμποδίσει τη διαβίβαση εμπιστευτικών πληροφοριών σε κακόβουλο τρίτο ή να εξασφαλισθεί η επιβεβαίωση ή απόδειξη εγκληματικών δράσεων του εργαζομένου. Σε κάθε περίπτωση προ της οιασδήποτε έρευνας ή ελέγχου ο εργαζόμενος καλείται εγγράφως με αιτιολογημένη πρόσκληση να καταθέσει τις απόψεις του σχετικά με τα εγειρόμενα ζητήματα, ενημερώνεται για το χρόνο στον οποίο αυτός θα λάβει χώρα, ενώ δικαιούται να ζητήσει να είναι παρών κατά τη διαδικασία ελέγχου νομικός συμπαραστάτης ή και τεχνικός σύμβουλος. Κατά την ολοκλήρωση της διαδικασίας ελέγχου ο εργαζόμενος δικαιούται να ζητήσει το πόρισμα αυτού όπως και να εκφράσει τις αντιρρήσεις και εν γένει τις απόψεις του επ' αυτού.

Το Π.Δ.Μ. θα εκμεταλλευτεί **την** Πολιτική Χρήσης Κινητών Συσκευών και Τηλεργασία.