ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

Προσχέδιο Πολιτικής Τηλεργασίας και Κινητών Συσκευών

Σκοπός (Purpose)

Σκοπός αυτής της πολιτικής είναι να δημιουργηθεί ένα πλαίσιο διαχείρισης με σκοπό να διασφαλιστεί η ασφάλεια της χρήσης φορητών συσκευών και της τηλεργασίας στο Πανεπιστήμιο Δυτικής Μακεδονίας. Η πολιτική αυτή έχει συνταχθεί σύμφωνα με τα προβλεπόμενα στο Παράρτημα Α6 του Διεθνούς Προτύπου Διαχείρισης Ασφάλειας της Πληροφορίας ISO27001:2013.

Αντικείμενο (Scope)/ Εξαιρέσεις (Exclusions)

Το αντικείμενο αυτής της πολιτικής περιλαμβάνει όλους τους **κανόνες αποδεκτής χρήσης** και τα **μέτρα προστασίας** που πρέπει να λαμβάνονται σχετικά με τη χρήση **φορητών συσκευών (portable devices)** που χρησιμοποιούνται για την πρόσβαση, επεξεργασία, αποθήκευση πληροφοριών – δεδομένων του Ιδρύματος καθώς και σχετικά με την **τηλεργασία**.

Στο πεδίο εφαρμογής της πολιτικής αυτής υπάγονται οι κάτωθι φορητές συσκευές[1]:

- Υπολογιστικά Συστήματα προσωπικής χρήσης του Ιδρύματος, εφόσον μεταφέρονται συστηματικά εκτός των κεντρικών εγκαταστάσεων του, εξαιρουμένων περιπτώσεων όπου μεταφέρονται μόνο για μιας μικρής διάρκειας συνάντηση στο πλαίσιο συνεδρίων, παρουσιάσεων, συνεργειών και άλλων δράσεων και επιστρέφουν στις εγκαταστάσεις του Ιδρύματος ή άλλης περιστασιακής απομάκρυνσης (πχ συντήρηση/επισκευή)
- Προσωπικές συσκευές, Handheld devices/ mobile devices (συσκευές χειρός/ κινητές συσκευές) όπως φορητοί υπολογιστές, προσωπικοί υπολογιστές, Tablets και Smartphones που χρησιμοποιούν δεδομένα και πληροφορίες του Ιδρύματος (συμπεριλαμβανομένης της σύνδεσης στο wi-fi intranet)
- Επίσης υπάγονται οι συσκευές που δεν ανήκουν στο Ίδρυμα αλλά χρησιμοποιούνται στο πλαίσιο της τηλεργασίας.

Σημειώσεις:

1) Laptops, που δεν μεταφέρονται συστηματικά εκτός των κεντρικών εγκαταστάσεων, αντιμετωπίζονται ως desktops. Για τη βιωσιμότητα της θεώρησης αυτής το Ίδρυμα τηρεί μητρώο υλικού που καταγράφεται η απομάκρυνση του εξοπλισμού από τις εγκαταστάσεις.
2) Δεν επιτρέπεται η χρήση ιδιόκτητων laptops και tablets για την εκτέλεση εργασιών του Ιδρύματος πλην των εξαιρέσεων κατόπιν έγκρισης από το Ίδρυμα. Στην περίπτωση αυτή εφαρμόζονται τα καθοριζόμενα στην § 6.1.9 .

Η παρούσα πολιτική αποτελείται από τις ακόλουθες επί μέρους πολιτικές:

- Πολιτική Ασφάλειας Φορητών Συσκευών (βλ. § 6.1)
- Πολιτική Τηλεργασίας (βλ. § 6.2)

Σε ποιους απευθύνεται – Πεδίο εφαρμογής

[1] Όπου ισχύουν διαφορετικοί κανόνες για τις συσκευές χειρός από τα laptops θα αναφέρεται ρητά, άλλως τα αναγραφόμενα ισχύουν και για τους 2 τύπους.

Το έγγραφο αυτό αποτελεί μέρος της συνολικής πολιτικής ασφαλείας του Πανεπιστήμιου Δυτικής Μακεδονίας και ως εκ τούτου πρέπει να τηρείται πλήρως.
Αυτή η πολιτική ισχύει για όλους τους υπαλλήλους και τους εξωτερικούς συνεργάτες με σταθερή συνεργασία με το Ίδρυμα.

Ορισμοί

Τηλεργασία - Το άρθρο 2 της Ευρωπαϊκής Συμφωνίας Πλαίσιο για την Τηλεργασία του 2002 ορίζει την τηλεργασία ως: «μια μορφή οργάνωσης ή / και εκτέλεσης εργασιών, χρησιμοποιώντας την τεχνολογία των πληροφοριών, στο πλαίσιο μιας σύμβασης / σχέσης εργασίας, όπου η εργασία, όπου η εργασία, που θα μπορούσε να εκτελεστεί στις εγκαταστάσεις του εργοδότη, εκτελείται τακτικά εκτός των εγκαταστάσεων αυτών» [2]
Εμπιστευτικές πληροφορίες – «οι πληροφορίες που αν αποκαλυφθούν ή χαθούν αδικαιολόγητα θα μπορούσαν να προκαλέσουν βλάβη ή οικονομικές απώλειες ή απώλεια φήμης για το Ίδρυμα. Αυτές περιλαμβάνουν προσωπικά δεδομένα, όπως ορίζονται από τον νόμο περί προστασίας δεδομένων, καθώς και άλλες πολύτιμες ή ευαίσθητες πληροφορίες που δεν είναι δημόσιες, όπως πληροφορίες που είναι εμπορικά εμπιστευτικές και πληροφορίες σχετικές με την πνευματική ιδιοκτησία.»
Κινητή συσκευή πληροφορικής – «μια φορητή συσκευή υπολογιστών ή τηλεπικοινωνιών που μπορεί να εκτελέσει προγράμματα ή να αποθηκεύσει ψηφιακά δεδομένα. Παραδείγματα: φορητός υπολογιστής, προσωπικός ψηφιακός βοηθός (PDA), έξυπνο τηλέφωνο, έξυπνος ρολόι και άλλοι φορητοί υπολογιστές, ψηφιακή φωτογραφική μηχανή, CD, DVD, εξωτερικός / αφαιρούμενος σκληρός δίσκος».

Παραπομπές και σχετιζόμενες πολιτικές ή άλλα έγγραφα

Παράρτημα «Ι»
Παράρτημα «ΙΙ»

Πολιτική φορητών συσκευών & τηλεργασίας

Η παρούσα ενότητα αφορά την δημιουργία ενός πλαισίου διαχείρισης για την διασφάλιση της ασφάλειας της τηλεργασίας και της χρήσης φορητών συσκευών.
Αποτελείται από τις ακόλουθες 2 υποενότητες:

- Πολιτική Ασφάλειας Φορητών Συσκευών (βλ. §6.1)
- Πολιτική Τηλεργασίας (βλ. §6.2)

Πολιτική Ασφάλειας Φορητών Συσκευών

Το Πανεπιστήμιο Δυτικής Μακεδονίας αποδέχεται την ανάγκη για υιοθέτηση πολιτικής και υποστηρικτικών μέτρων ασφάλειας για τη διαχείριση των κινδύνων που δημιουργούνται με τη χρήση έξυπνων κινητών τηλεφώνων και άλλων φορητών συσκευών όπως φορητοί υπολογιστές, tablet κ.λπ. Στόχος της υποενότητας αυτής είναι η εξασφάλιση την προστασίας και του ελέγχου των πληροφοριακών αγαθών όταν χρησιμοποιούνται φορητές συσκευές ή το προσωπικό εργάζεται εκτός των εγκαταστάσεων υποστηρίζοντας άμεσα ή έμμεσα τις δραστηριότητες του Ιδρύματος. Στο πλαίσιο αυτό:

1. Η αποθήκευση όσο το δυνατόν λιγότερων πληροφοριών στις φορητές συσκευές είναι ο καλύτερος τρόπος να διασφαλιστεί ότι δεν θα κλαπεί διαβαθμισμένη πληροφορία.

[2] Σημείωση: Η τηλεργασία μπορεί να περιλαμβάνει ποικίλες ρυθμίσεις εργασίας, όπως εργασία στο σπίτι, εργασία από γραφεία σε διαφορετικές τοποθεσίες κ.α. Οι τηλεργαζόμενοι μπορεί να είναι υπάλληλοι της εταιρείας ή αυτοαπασχολούμενοι.

2. Το Ίδρυμα ορίζει ως αποδεκτή προσωπική χρήση κατά το ωράριο απασχόλησης μια εύλογα περιορισμένη προσωπική επικοινωνία ή αναψυχή, όπως η ανάγνωση ειδήσεων ή η χρήση μέσων κοινωνικής δικτύωσης.
3. Οι χρήστες φορητών συσκευών πρέπει να προστατεύουν με επιμέλεια αυτές τις συσκευές από απώλεια και από αποκάλυψη διαβαθμισμένης πληροφορίας που ανήκει ή τηρείται στο Πανεπιστήμιο Δυτικής Μακεδονίας.
4. Τα Τμήματα Μηχανοργάνωσης/Πληροφορικής και Δικτύων πρέπει να ενημερώνονται αμέσως μετά από υποψία συμβάντος ασφαλείας, ιδίως όταν μια φορητή συσκευή μπορεί να έχει χαθεί ή κλαπεί. Για μια τηλεφωνική συσκευή που ανήκει στον εργαζόμενο, εκείνος έχει την ευθύνη για την ειδοποίηση του φορέα κινητής τηλεφωνίας αμέσως μετά την απώλεια της συσκευής. Για μια φορητή υπολογιστική μηχανή που ανήκει στον εργαζόμενο, εκείνος έχει την ευθύνη για απομακρυσμένη διαγραφή των δεδομένων.
5. Ο εργαζόμενος αναμένεται να χρησιμοποιεί τις φορητές συσκευές του με ηθικό τρόπο. Οι συσκευές δεν μπορούν να χρησιμοποιηθούν σε καμία χρονική στιγμή για:
    a. αποθήκευση ή μετάδοση παράνομων υλικών
    b. αποθήκευση ή μετάδοση πληροφοριών που ανήκουν σε τρίτο χωρίς την άδεια αυτού
    c. ενόχληση τρίτων
    d. άσκηση δραστηριοτήτων εκτός επιχείρησης, εάν η συσκευή είναι εταιρική
6. Ο εργαζόμενος ευθύνεται προσωπικά για φθορές που σχετίζονται με τη συσκευή του, εάν η συσκευή είναι του Ιδρύματος
7. Ειδικά για τις συσκευές χειρός (handheld devices):
    a. Στις συσκευές χειρός εν γένει **ΔΕΝ** αποθηκεύονται δεδομένα του Ιδρύματος, ούτε πρέπει να χρησιμοποιούνται για την πρόσβαση στα folders του Ιδρύματος, μπορούν όμως να συνδέονται στο δίκτυο του για οποιαδήποτε αποδεκτή χρήση περιγράφεται στη συνέχεια, και πάντα σε συμμόρφωση με την παρούσα πολιτική.
    b. Οι εργαζόμενοι μπορούν να χρησιμοποιήσουν τη συσκευή για να αποκτήσουν πρόσβαση στους ακόλουθους πόρους: ηλεκτρονικό ταχυδρομείο, ημερολόγιο, επαφές, δίκτυο του Ιδρύματος
8. Το Πανεπιστήμιο Δυτικής Μακεδονίας εφαρμόζει πολιτική μηδενικής ανοχής για την πληκτρολόγηση ή την αποστολή μηνυμάτων κατά την οδήγηση όπου επιτρέπεται μόνον ομιλία χωρίς χρήση χεριών (hands-free).

Το Πανεπιστήμιο Δυτικής Μακεδονίας αντιλαμβάνεται την ανάγκη εφαρμογής μιας στρατηγικής "Άμυνας Βάθους" με συνδυασμό συμπληρωματικών φυσικών, τεχνικών και πολιτικών ελέγχων. Μία από τις σημαντικότερες πτυχές της ασφάλειας των φορητών συσκευών είναι η εκπαίδευση, η κατάρτιση και η ευαισθητοποίηση σχετικά με τη χρήση κινητών συσκευών σε δημόσιους χώρους, αποφεύγοντας τον κίνδυνο που γεννάται από την άμεση χρήση του «δημόσιου» wi-fi που θα μπορούσε να διακυβεύσει την ασφάλεια πληροφοριών. Παράλληλα ο καθορισμός κανόνων σε πρακτικές «Bring Your Own Device – BYOD» στις ειδικές περιπτώσεις των εξωτερικών συνεργατών και εργαζομένων αποτελεί μια ακόμη γραμμή άμυνας και προστασίας των πληροφοριακών αγαθών.

Η πολιτική των φορητών συσκευών εξετάζει τα ακόλουθα:

1. εγγραφή και διαχείριση των συσκευών
2. θέματα φυσικής προστασίας
3. περιορισμούς της εγκατάστασης λογισμικών
4. ενημερώσεις λειτουργικών συστημάτων και εφαρμογών

5. περιορισμούς σύνδεσης
6. ελέγχους – περιορισμούς πρόσβασης
7. προστασία από κακόβουλα λογισμικά
8. αντίγραφα ασφαλείας και αποθήκευση
9. συνθήκες πρόσβασης χρηστών με πρακτικές BYOD

Αναλυτικότερα τα θέματα αυτά ακολουθούν.

Εγγραφή και Διαχείριση των Συσκευών

Η καταχώρηση των πανεπιστημιακών φορητών συσκευών γίνεται με μέριμνα των Τμημάτων Μηχανοργάνωσης/Πληροφορικής και Δικτύων.

Θέματα Φυσικής Προστασίας

Οι φορητές συσκευές λόγω της φορητής φύσης τους, δημιουργείται αυξημένος κίνδυνος κλοπής ή απώλειας. Συνεπώς, στο πλαίσιο της φυσικής προστασίας από απώλεια ή κλοπή πρέπει να τηρούνται οι εξής προφυλάξεις:

1. Οι φορητές συσκευές να μην αφήνονται εκτός Πανεπιστημίου καμία στιγμή χωρίς την επιτήρηση - εποπτεία του κατόχου ή κάποιου συναδέλφου του για το οποίο υφίσταται εμπιστοσύνη.
2. Οι φορητές συσκευές να μην αφήνονται αφύλακτες, ούτε για μικρό διάστημα, σε αυτοκίνητα και ιδίως σε θέση ορατή από έξω
3. Να μην αφήνονται σε χώρο εργασίας άλλων, μετά το πέρας του ωραρίου απασχόλησης. Εξαιρέσεις αποτελούν περιπτώσεις που στον παραπάνω χώρο εργασίας υφίστανται αποδεδειγμένα ενισχυμένα μέτρα ασφάλειας, τα οποία περιλαμβάνουν κατ' ελάχιστον κλείδωμα γραφείων, 24ωρη φύλαξη κτιρίων και κλειστό κύκλωμα επιτήρησης περιβαλλόντων χώρων.

Περιορισμοί εγκατάστασης Λογισμικών

Απαγορεύεται:

1. Η εγκατάσταση και χρήση μη εξουσιοδοτημένων εφαρμογών ή υπηρεσιών στις φορητές συσκευές. Σε περίπτωση που αυτό κριθεί απαραίτητο να ζητείται η γνώμη των Τμημάτων Μηχανοργάνωσης/Πληροφορικής και Δικτύων και του Ιδιοκτήτη του αγαθού.
2. Η εγκατάσταση εφαρμογών που δεν είναι αποδεδειγμένα απαραίτητες για την εκπλήρωση των καθηκόντων του χρήστη.
3. Ειδικά για τις συσκευές χειρός, δεν πρέπει να πραγματοποιείται download εφαρμογής που δεν προέρχεται από έμπιστη πηγή όπως τα επίσημα καταστήματα Apple Store ή Google Play ή Windows Marketplace.

Τα Τμήματα Μηχανοργάνωσης/Πληροφορικής και Δικτύων πρέπει να τηρούν λίστα με τις επιτρεπόμενες και μη εφαρμογές την οποία κάνουν διαθέσιμες στους χρήστες του Ιδρύματος στο intranet.

Προκειμένου να ενισχυθεί το επίπεδο ασφάλειας των τελικών συσκευών, όλες οι μη απαραίτητες διαδικτυακές υπηρεσίες/ εφαρμογές δεν θα πρέπει να είναι εγκατεστημένες ή ενεργοποιημένες. Συγκεκριμένα απαγορεύεται η εγκατάσταση εφαρμογών/υπηρεσιών που παρέχουν ιδίως:

1. Internet file-sharing
2. FTP client
3. Peer-to-peer services (e.g. BitTorrent)
4. Instant messaging εφαρμογές πλην των εγκεκριμένων (π.χ. Skype)
5. Πλοήγηση με δυνατότητα ανωνυμίας (π.χ. tor)

6. Οποιοσδήποτε τύπος tunneling εφαρμογής που δεν επιτρέπει content filtering της επικοινωνίας, με εξαίρεση την εγκεκριμένη εταιρική **VPN ή remote desktop** διασύνδεση.

- Τα Τμήματα Μηχανοργάνωσης/Πληροφορικής και Δικτύων εκδίδουν λίστα με τις απαραίτητες υπηρεσίες και εφαρμογές που πρέπει και μόνο να είναι ενεργοποιημένες και θα τις κοινοποιούν στους τελικούς χρήστες. Οι χρήστες μπορούν να απευθύνονται στα Τμήματα Μηχανοργάνωσης/Πληροφορικής και Δικτύων για τεχνική υποστήριξη στην ενεργοποίηση και απενεργοποίηση των υπηρεσιών και λειτουργιών.

Ενημερώσεις Λειτουργικών Συστημάτων & Εφαρμογών

1. Οι συσκευές πρέπει να διαθέτουν τις τελευταίες ενημερώσεις ασφαλείας των Λειτουργικών Συστημάτων. Για τυχόν άλλες ενημερώσεις και αναβαθμίσεις πρέπει να ζητούν τη γνώμη των Τμημάτων Μηχανοργάνωσης/Πληροφορικής και Δικτύων διότι ενδέχεται η επικείμενη αναβάθμιση να οδηγήσει σε άρνηση υπηρεσιών του Ιδρύματος. Η ενημέρωση του Λειτουργικού Συστήματος των συσκευών χειρός/κινητών συσκευών αποτελεί ευθύνη του χρήστη.
2. Οι εφαρμογές πρέπει να ενημερώνονται με τα πιο πρόσφατα patches προκειμένου να αποφευχθούν οι ευπάθειες και να γίνει πιο σταθερή η συσκευή.
3. Το firmware των συσκευών χειρός πρέπει να ενημερώνεται σε τακτική βάση προκειμένου να αποφευχθούν οι ευπάθειες και να γίνει πιο σταθερή η συσκευή. Η ενημέρωση είναι ευθύνη του χρήστη.

Περιορισμοί Σύνδεσης (Χρήση σε Δημόσιους Χώρους & Πρόσβαση σε Μη Αξιόπιστα Δίκτυα)

1. Πρέπει να επιδιώκεται ελαχιστοποίηση της χρήσης δημόσιων ασύρματων δικτύων (wi-fi), όπως π.χ. στα ανοιχτά / μη προστατευμένης πρόσβασης wi-fi σε αεροδρόμια, ξενοδοχεία και καφετέριες.
2. Εάν πρέπει να χρησιμοποιηθεί ένα wi-fi hotspot εκτός ελέγχου του Ιδρύματος, θα πρέπει να αποφευχθεί η διακίνηση εμπιστευτικών/ευαίσθητων δεδομένων. Ωστόσο, όπου υφίσταται συχνή ανάγκη διακίνησης εμπιστευτικών/ευαίσθητων δεδομένων ενώ ο χρήστης βρίσκεται εν κινήσει, για την εξασφάλιση υψηλού επιπέδου προστασίας αναφορικά με τη σύνδεση του χρήστη της φορητής συσκευής σε πανεπιστημιακά αγαθά θα πρέπει να λαμβάνονται υπόψη οι οδηγίες του Παραρτήματος «Ι».

Έλεγχοι - Περιορισμοί Πρόσβασης

Διαδικασία Εισόδου, Απομακρυσμένος Έλεγχος και Εντοπισμός

Το Πανεπιστήμιο Δυτικής Μακεδονίας χορηγεί περιορισμένο αριθμό φορητών συσκευών χειρός (smartphones, tablets) σε συγκεκριμένα ανώτερα στελέχη, στις οποίες εν γένει δεν αποθηκεύονται δεδομένα, πέραν της δυνατότητας πρόσβασης στα emails και στα τυχόν επισυναπτόμενα αρχεία. Για την είσοδο στις φορητές συσκευές πρέπει να εφαρμόζονται από όλους τα κάτωθι σημεία ελέγχου πρόσβασης:

1. Ρύθμιση κλειδώματος οθόνης (lock screen). Πέραν του κωδικού ανοίγματος/ξεκλειδώματος, εφόσον διατίθεται δυνατότητα αναγνώρισης δακτυλικού αποτυπώματος, συστήνεται να χρησιμοποιείται αυτή η μέθοδος για το άνοιγμα της οθόνης.
2. Αυτόματο κλείδωμα με password ή PIN για διάστημα αδράνειας μεγαλύτερο από 5 λεπτά στα laptops και 1 λεπτό στις συσκευές χειρός.
3. Επειδή οι συσκευές Bluetooth είναι πολύ εύκολο να "ανακαλύπτονται", να συνδέονται με άλλες συσκευές και δυνητικά να «χακάρονται», συστήνεται ρύθμιση της συσκευής Bluetooth στην κρυφή λειτουργία (hidden mode) και ενεργοποίηση Bluetooth μόνο όταν χρειάζεται.

Ανήκει στις προτεραιότητες του Ιδρύματος η μελλοντική αξιοποίηση δυνατότητας κεντρικού remote wipe-out, κλειδώματος και εντοπισμού της συσκευής ανάλογα με τη τεχνολογία της φορητής συσκευής. Προς το παρόν αυτό εξασφαλίζεται μόνο για τα έξυπνα κινητά τηλεφωνά και τα tablets με χρήση του λογαριασμού χρήστη (find my iphone, find my device - android).

Περιορισμοί Πρόσβασης σε Πληροφορίες και Κρυπτογράφηση

1. για φορητούς υπολογιστές

Οποιαδήποτε δεδομένα αποθηκεύονται τοπικά στη συσκευή που χαρακτηρίζονται απόρρητα (αυστηρά εμπιστευτικά) ή αφορούν προσωπικά δεδομένα τρίτων θα πρέπει να κρυπτογραφούνται, προκειμένου να αποφευχθεί η κλοπή δεδομένων και η αποκάλυψη σε τρίτους. Για το σκοπό αυτό θα αξιοποιείται διακριτό partition, το οποίο θα διαμορφώνεται κατά το αρχικό setup του υπολογιστή από τα Τμήματα Μηχανοργάνωσης/Πληροφορικής και Δικτύων. Για την κρυπτογράφηση μπορεί να χρησιμοποιείται η εφαρμογή Bitlocker που παρέχεται εγγενώς από το λειτουργικό σύστημα ή άλλης εγκεκριμένης από τα Τμήματα Μηχανοργάνωσης/Πληροφορικής και Δικτύων εφαρμογής.

Η ίδια πολιτική (κρυπτογράφηση με χρήση της ανωτέρω εφαρμογής) θα ακολουθείται για την αποθήκευση απόρρητων (αυστηρά εμπιστευτικά) ή προσωπικών δεδομένων τρίτων σε οποιοδήποτε αφαιρούμενο αποθηκευτικό μέσο (π.χ. usb sticks).

2. για συσκευές χειρός

Απόρρητα και εμπιστευτικά έγγραφα **ΔΕΝ** πρέπει να αποθηκεύονται σε συσκευές χειρός, εκτός αν παραστεί απόλυτη ανάγκη και σε αυτήν την περίπτωση θα πρέπει να διαγραφούν το συντομότερο δυνατόν.

Προστασία από Κακόβουλα Λογισμικά

Αναφορικά με τη προστασία των φορητών συσκευών από κακόβουλες εφαρμογές, αυτές θα διαθέτουν εγκατεστημένο λογισμικό προστασίας από ιούς. Ειδικότερα:

1. Τα laptops φέρουν προεγκατεστημένο το λογισμικό antivirus που χρησιμοποιεί το Πανεπιστήμιο, το οποίο ενημερώνεται αυτόματα σε διαρκή βάση
2. Στις συσκευές χειρός η εγκατάσταση σχετικού λογισμικού antivirus γίνεται με ευθύνη του χρήστη, ο οποίος βέβαια πρέπει να απευθύνεται στα Τμήματα Μηχανοργάνωσης/Πληροφορικής και Δικτύων.

Αντίγραφα Ασφαλείας και Αποθήκευση

Ο υπάλληλος ή εξωτερικός συνεργάτης είναι προσωπικά υπεύθυνος για την ασφαλή δημιουργία αντιγράφων ασφαλείας οποιονδήποτε δεδομένων τηρούνται τοπικά, που σχετίζονται με την άσκηση πανεπιστημιακών δραστηριοτήτων, μέχρις ότου αυτά τα δεδομένα αποθηκευτούν στο δίκτυο του Ιδρύματος όπου το backup υποστηρίζεται συστηματικά.

Θέση για την λήψη αντιγράφων ασφαλείας:

1. Κατά την εργασία στις εγκαταστάσεις του Ιδρύματος:
    - Στον προσωπικό χώρο που έχει ο κάθε χρήστης στο εσωτερικό δίκτυο του Ιδρύματος
    - Στα κατάλληλα folders του εσωτερικού δικτύου μόλις αυτά καταστούν διαθέσιμα.
2. Κατά την εργασία εκτός των εγκαταστάσεων του Ιδρύματος, και κατά σειρά προτεραιότητας:
    - Στα κατάλληλα folders του εσωτερικού δικτύου εάν υπάρχει διαθέσιμη VPN connection μέσω ασφαλούς σύνδεσης ή σύνδεση απομακρυσμένης επιφάνειας εργασίας
    - Σε κάθε άλλο πρόσφορο μέσο (π.χ. usb sticks) με την επιφύλαξη της § 6.1.6

Πρόσβαση Χρηστών με Πρακτικές BYOD

Με τον όρο Bring Your Own Device εννοείται πρακτική, με βάση την οποία οι υπάλληλοι ενός οργανισμού χρησιμοποιούν, για επιχειρησιακούς λόγους, ιδιόκτητες συσκευές (έξυπνα τηλέφωνα, tablets, φορητούς υπολογιστές και άλλες πλατφόρμες) για πρόσβαση σε εσωτερικές εφαρμογές, όπως ηλεκτρονικό ταχυδρομείο και βάσεις δεδομένων, αλλά και για δημιουργία, αποθήκευση και διαχείριση δεδομένων.

Οι πρακτικές BYOD κατά κανόνα δεν λαμβάνουν χώρα στο Πανεπιστήμιο. Εξαιρέσεις στον κανόνα αυτόν αποτελούν:

1. τα έξυπνα κινητά τηλέφωνα των εργαζομένων
2. περιορισμένες περιπτώσεις φορητών υπολογιστών εξωτερικών συνεργατών ή εργαζομένων που εργάζονται συστηματικά από μακριά.
3. Περιπτώσεις εργαζομένων που εργάζονται στο πλαίσιο της τηλεργασίας σε ειδικές περιπτώσεις (π.χ. επιδημίας, φυσικών καταστροφών, ανωτέρας βίας, κ.α)

Για αυτές τις περιπτώσεις το Πανεπιστήμιο πρέπει εφαρμόζει τα ακόλουθα μέτρα:

1. Προστασία των πληροφοριακών αγαθών που είναι σε επικοινωνία με το διακομιστή / server ή οποιαδήποτε άλλη συσκευή στο δίκτυο του Ιδρύματος, σε επίπεδο ανίχνευσης virus/malware ή οποιουδήποτε άλλου κακόβουλου κώδικα μέσω κεντρικής πλατφόρμας.
2. Κρυπτογραφημένη σύνδεση και επικοινωνία μέσω π.χ. SSL/IPSEC/VPN, μεταξύ client/ server για τους «roaming users» με χρήση του VPN του Ιδρύματος.
3. Κρυπτογραφημένη σύνδεση και επικοινωνία μέσω απομακρυσμένη επιφάνειας εργασίας
4. Υποχρέωση από μεριάς των χρηστών για:
    a. Αποθήκευση δεδομένων με Κρυπτογράφηση
    b. Προστασία από ιομορφικό λογισμικό με κατάλληλη εφαρμογή
    c. Υποχρεωτική δήλωση συσκευής στα Τμήματα Μηχανοργάνωσης/Πληροφορικής και Δικτύων στην περίπτωση της τηλεργασίας
    d. Έλεγχος συμμόρφωσης ρυθμίσεων συσκευών με πολιτική BYOD
5. Ύπαρξη Τείχους προστασίας στις κεντρικές εφαρμογές και τα δίκτυα.
6. Για τις κινητές έξυπνες συσκευές εφαρμογή λύσης Anti-Theft ή Remote Wipe, για την προστασία των δεδομένων σε περίπτωση απώλειας/κλοπής εκ μέρους των χρηστών.
7. Υποστήριξη χρηστών/συσκευών (έστω συμβουλευτικά)
8. Υπό διερεύνηση τελεί η εξέταση και υιοθέτηση:
    a. Εφαρμογής ειδικών φίλτρων ανίχνευσης δικτυακής κίνησης τύπου IDS/IPS.
    b. Η εγκατάσταση Συστήματος Πληροφόρησης Γεγονότων Συστημάτων (SIEM).
    c. Επιβολή πολιτικών ασφαλείας στους φορητούς υπολογιστές κατά την είσοδο τους στο εσωτερικό δίκτυο του Ιδρύματος.
    d. Απενεργοποίηση λειτουργιών με βάση τοποθεσία (geofencing)

Πολιτική Τηλεργασίας

Κατά κανόνα δεν υφίσταται προσωπικό που εργάζεται συστηματικά από μακριά. Εξαιρέσεις εδώ αποτελούν:

- Εργαζόμενοι που περιστασιακά βρίσκονται εκτός εγκαταστάσεων (π.χ. σε ταξίδι ακαδημαϊκών συναντήσεων, short-term missions, συναντήσεις εργασίας κ.α.)
- Εξωτερικοί συνεργάτες που εργάζονται από το χώρο τους.
- Εργαζόμενοι που βρίσκονται για συγκεκριμένους λόγους σε εγκαταστάσεις άλλων.

- Εργαζόμενοι που για λόγους ανωτέρας βίας (π.χ. πανδημία) ή λόγους υγείας δεν μπορούν να εργαστούν από τον χώρο του Ιδρύματος.

Για τις ανωτέρω περιπτώσεις το Ίδρυμα εφαρμόζει συγκεκριμένη πολιτική και υποστηρικτικά μέτρα ως εξής:

1. Κατά κανόνα απαγορεύεται η πρόσβαση σε υπηρεσίες από μακριά.
2. Για το προσωπικό τηλεργασίας, η εκπαίδευση, η κατάρτιση και η ευαισθητοποίηση σχετικά με τους δυνητικούς κινδύνους είναι κρίσιμης σημασίας.
3. Τα μέτρα που λαμβάνονται στην περίπτωση της τηλεργασίας παρουσιάζονται στο Παράρτημα «ΙΙ»

Παραβίαση πολιτικής

Παραβιάσεις αυτής της πολιτικής ή/και συμβάντα/περιστατικά ασφαλείας μπορούν να οριστούν ως γεγονότα που θα μπορούσαν να οδηγήσουν ή έχουν οδηγήσει σε παραβίαση των διαδικασιών και των επιταγών του Πανεπιστημίου σχετικά με την οργάνωση της ασφάλειας της πληροφορίας και την ασφάλεια των φορητών συσκευών και επιφέρει πιθανή ή βεβαιωμένη απώλεια ή ζημιά στα αγαθά του ή σε ένα γεγονός που παραβιάζει άλλες διαδικασίες και πολιτικές ασφαλείας αυτού.

Όλοι οι εργαζόμενοι, τα μέλη Διοίκησης και οι εξωτερικοί συνεργάτες με σταθερή συνεργασία έχουν ευθύνη να αναφέρουν τα περιστατικά ασφαλείας και τις παραβιάσεις αυτής της πολιτικής το συντομότερο δυνατό σύμφωνα με τις **Οδηγίες ασφάλειας Πανεπιστημίου Δυτικής Μακεδονίας για την τηλεργασία** του Παραρτήματος «Ι» της παρούσας πολιτικής.

Το Πανεπιστήμιο Δυτικής Μακεδονίας θα λάβει τα κατάλληλα μέτρα για να διορθώσει τυχόν παραβίαση της πολιτικής και των συναφών διαδικασιών και κατευθυντήριων γραμμών μέσω των σχετικών προβλεπόμενων ενεργειών. Στην περίπτωση υπαλλήλου το θέμα μπορεί να αντιμετωπιστεί στο πλαίσιο των πειθαρχικών διαδικασιών και μπορεί να επισείει μέχρι και διακοπή συνεργασίας.

Έντυπα που χρησιμοποιούνται από την Πολιτική

- Ουδένα

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

▪

ΠΑΡΑΡΤΗΜΑΤΑ

Παράρτημα Ι: Οδηγίες χρήσης mobile devices & τηλεργασίας προς εργαζόμενους

Οδηγίες ασφάλειας Πανεπιστημίου Δυτικής Μακεδονίας για την τηλεργασία

Διαβάστε τις παρακάτω οδηγίες για να βεβαιωθείτε ότι έχετε κατανοήσει την ασφάλεια τηλεργασίας του Πανεπιστημίου Δυτικής Μακεδονίας

1. Θα ακολουθήσω καλές πρακτικές ασφάλειας πληροφοριών ως εξής:
    i. Θα αποφύγω την αποθήκευση κωδικών πρόσβασης: Η προσωρινή αποθήκευση κωδικών πρόσβασης στις κινητές συσκευές θα πρέπει να αποφεύγεται εάν είναι δυνατόν. Αυτό σημαίνει ότι δεν θα πρέπει να επιλέγω το πλαίσιο ελέγχου "Αποθήκευση κωδικού πρόσβασης" σε έναν ιστότοπο ή μια οθόνη εφαρμογής που ζητά τα διαπιστευτήρια σας.
    ii. Αν αποφασίσω να αποθηκεύσω προσωρινά έναν κωδικό πρόσβασης σε μια κινητή συσκευή, θα βεβαιωθώ πρώτα ότι προστατεύω τη συσκευή με κωδικό πρόσβασης.
    iii. Θα προστατέψω το smartphone ή το tablet μου με έναν κωδικό πρόσβασης. Η ενεργοποίηση της προστασίας με κωδικό πρόσβασης είναι η πιο κρίσιμη απαίτηση ασφαλείας που πρέπει να ακολουθήσω εάν χρησιμοποιώ το smartphone ή το tablet μου στην τηλεργασία μου.
    iv. Η ενεργοποίηση ενός κωδικού πρόσβασης στην φορητή μου συσκευή θα πρέπει επίσης να περιλαμβάνει μια ρύθμιση χρονοκαθυστέρησης για να κλειδώσει η συσκευή (απαιτεί έναν κωδικό πρόσβασης ξανά) μετά από μια παρατεταμένη περίοδο μη δραστηριότητας. Δεκαπέντε λεπτά θεωρείται γενικά μια καλή χρονική περίοδος.
    v. Θα απενεργοποιήσω το Bluetooth εάν δεν το χρησιμοποιώ
    vi. Θα προστατεύσω τον εξοπλισμό από την κλοπή όταν δεν χρησιμοποιείται. Εάν χάσω μια συσκευή που χρησιμοποίησα στην τηλεργασία μου:
        1. Αν η φορητή συσκευή μου λείπει και υποψιάζομαι ότι μπορεί να έχει πέσει σε χέρια κάποιου άλλου, πρέπει να λάβω μέτρα για την προστασία των πληροφοριών του Πανεπιστημίου.
        2. Θα ενημερώστε άμεσα τον άμεσα προϊστάμενο μου και τα Τμήματα Μηχανοργάνωσης/Πληροφορικής και Δικτύων.
        3. Θα αλλάξω οποιονδήποτε κωδικό πρόσβασης έχω στη συσκευή σας
2. Θα χρησιμοποιώ εξοπλισμό που χορηγείται από το Πανεπιστήμιο όποτε είναι δυνατόν.
3. Είναι δική μου ευθύνη να διασφαλίσω ότι ο προσωπικός εξοπλισμός που χρησιμοποιώ για την τηλεργασία θα πληροί όλες τις απαιτήσεις ασφαλείας όπως:
    i. Κρυπτογράφηση όλων των μέσων (π.χ. εσωτερικοί σκληροί δίσκοι, εξωτερικοί σκληροί δίσκοι, μονάδες flash).
    ii. Ενεργοποίηση των λειτουργιών ασφαλείας (π.χ. κωδικούς πρόσβασης, κλειδαριές οθόνης, απομακρυσμένη διαγραφή).
    iii. Ενεργοποίηση όλων των ενημερώσεων ασφαλείας για το λειτουργικό σύστημα, την ασφάλεια εφαρμογών και το κακόβουλο λογισμικό

4. Δεν θα μοιραστώ εξοπλισμό που δίδεται από πανεπιστήμιο ή χρησιμοποιώ στο πλαίσιο της τηλεργασίας (π.χ. με άλλα μέλη της οικογένειας). Αν αυτό δεν είναι εφικτό θα χρησιμοποιήσω διαφορετικό λογαριασμό χρήστη.
5. Θα προστατεύσω όλα τα φυσικά αρχεία που χρησιμοποιώ στην τηλεργασία μου από μη εξουσιοδοτημένη πρόσβαση.
6. Θα συνδεθώ μέσω VPN ή εγκεκριμένης εφαρμογής απομακρυσμένης επιφάνειας εργασίας πριν από την απομακρυσμένη σύνδεση στα πανεπιστημιακά συστήματα.
7. Θα αποθηκεύσω όλες τις πληροφορίες στους Πανεπιστημιακούς εξυπηρετητές όποτε είναι δυνατόν. Εάν δεν είναι δυνατόν, επιτρέπεται η προσωρινή αποθήκευση μη περιορισμένων δεδομένων σε προστατευμένες με κωδικό πρόσβασης και κρυπτογραφημένες κινητές συσκευές ή φακέλους.
8. Δεν θα χρησιμοποιήσω δημόσιες υπολογιστικές μηχανές ή δημόσια δίκτυα για να συνδεθώ σε πανεπιστημιακά συστήματα και δεν θα χρησιμοποιήσω κωδικούς πρόσβασης που χρησιμοποιούνται σε δημόσια μηχανήματα ή για άλλους σκοπούς.
9. Θα εξοικειωθώ με τις ειδοποιήσεις ηλεκτρονικού "ψαρέματος" και αδυναμιών και θα επισκεφτώ για να μελετήσω για το phishing στην διεύθυνση **https://cert.grnet.gr/el/οδηγίες-2/s**
10. Θα αναφέρω αμέσως όλες τις παραβιάσεις ασφάλειας της τεχνολογίας της πληροφορικής ή του εξοπλισμού καλώντας στο XXXXXX κατά τις συνήθεις ώρες εργασίας ή στέλνοντας email XXXXXX έξω από τις συνήθεις ώρες εργασίας.
11. Μπορώ να επιλέξω να μην κάνω χρήση της κάμερας κατά την διάρκεια τηλεδιασκέψεων με τηλεργασία.
12. Θα προσέξω να κλείνω το μικρόφωνο μου όταν δεν μιλάω κατά την διάρκεια τηλεδιασκέψεων με τηλεργασία.

Ημερομηνία Υπογραφής Εργαζομένου	
Ονοματεπώνυμο Εργαζόμενου	

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

Παράρτημα ΙΙ: Μέτρα Ασφαλείας τηλεργασίας

Πρόσβαση στο δίκτυο

ΑΠΑΙΤΗΣΗ	ΤΡΟΠΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ
1. Διασφάλιση ότι δεν υπάρχει δυνατότητα μη ασφαλούς απομακρυσμένης πρόσβασης σε πόρους των πληροφοριακών συστημάτων του φορέα, όπως υπολογιστές εσωτερικού δικτύου και εσωτερικά αρχεία. Η ασφαλής σύνδεση μπορεί, ενδεικτικώς, να επιτευχθεί μέσω εικονικού ιδιωτικού δικτύου στο οποίο πραγματοποιείται κρυπτογράφηση των δεδομένων και αυθεντικοποίηση τωνχρηστών (π.χ. IPSec VPN).	
i. Καθορισμός και περιορισμός των πόρων στους οποίους επιτρέπεται η απομακρυσμένη πρόσβαση στο απολύτως απαραίτητο, ανάλογα με τα καθήκοντα που επιτελεί ο τηλεργαζόμενος.	
ii. Σύνδεση σε υπολογιστικά συστήματα του φορέα μέσω υπηρεσίας “απομακρυσμένης επιφάνειας εργασίας” (“Remote Desktop Protocol - RDP”), μόνο εφόσον αυτή γίνεται μέσω ασφαλούς εικονικού ιδιωτικού δικτύου (VPN).	
2. Χρήση ασφαλούς πρωτοκόλλου WPA2 με ισχυρό κωδικό, όταν η σύνδεση της συσκευής του τηλεργαζόμενου στο Διαδίκτυο γίνεται μέσω ασύρματου δικτύου (Wi-Fi). Τούτο ισχύει ακόμα και όταν μετά τη σύνδεση στο Διαδίκτυο, γίνεται ασφαλής σύνδεση στο δίκτυο του φορέα π.χ. με χρήση VPN.	
3. Αποφυγή αποθήκευσης αρχείων με προσωπικά δεδομένα σε υπηρεσίες διαδικτυακής αποθήκευσης (π.χ. Dropbox, One Drive, google drive), εκτός και αν υπάρχουν τα κατάλληλα εχέγγυα, όπως π.χ. να πρόκειται για υπηρεσία που παρέχεται, με κατάλληλα μέτρα ασφάλειας, από τον φορέα ή τα δεδομένα να αποθηκεύονται αποκλειστικά σε κατάλληλα κρυπτογραφημένη μορφή.	

Χρήση εφαρμογών ηλεκτρονικού ταχυδρομείου/ανταλλαγής μηνυμάτων

ΑΠΑΙΤΗΣΗ	ΤΡΟΠΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ
1. Αποφυγή χρήσης προσωπικού ηλεκτρονικού ταχυδρομείου (π.χ. gmail, yahoo, hotmail) για αποστολή ή λήψη μηνυμάτων για σκοπούς τηλεργασίας, τα οποία σχετίζονται με προσωπικά δεδομένα. Αντ’ αυτού, θα πρέπει να χρησιμοποιείται η επαγγελματική ηλεκτρονική διεύθυνση την οποία παρέχει ο φορέας. Εάν αυτό δεν είναι τεχνικά εφικτό (π.χ. μη δυνατότητα πρόσβασης στο εσωτερικό ηλεκτρονικό ταχυδρομείο από εξωτερικό του φορέα δίκτυο), τότε το περιεχόμενο των μηνυμάτων που αφορά προσωπικά δεδομένα πρέπει να κρυπτογραφείται κατάλληλα (π.χ. είτε ολόκληρο το μήνυμα είτε μόνο τα συνημμένα αρχεία).	

2. Αποφυγή χρήσης εφαρμογών ανταλλαγής μηνυμάτων (κείμενο ή/και βίντεο) για τους σκοπούς της τηλεργασίας, όταν τα μηνύματα αυτά περιέχουν προσωπικά δεδομένα, των οποίων τυχόν διαρροή θα επέφερε κινδύνους. Αν είναι πραγματικά απαραίτητο, να προτιμώνται υπηρεσίες των οποίων τα χαρακτηριστικά ασφάλειας (κρυπτογράφηση, ρυθμίσεις προστασίας δεδομένων) αξιολογούνται ως ισχυρά.	

Χρήση τερματικής συσκευής\αποθηκευτικών μέσων

ΑΠΑΙΤΗΣΗ	ΤΡΟΠΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ
1. Εγκατάσταση και τακτική ενημέρωση αντιϊκού προγράμματος και "αναχώματος ασφαλείας" (firewall) στη συσκευή (π.χ. υπολογιστής, laptop κτλ.) μέσω της οποίας πραγματοποιείται η τηλεργασία.	
2. Εγκατάσταση των πλέον πρόσφατων ενημερώσεων του λογισμικού εφαρμογών και λειτουργικού συστήματος της συσκευής των εργαζομένων.	
3. Χρήση προγραμμάτων πλοήγησης στο Διαδίκτυο (π.χ. Firefox, Chrome κτλ.) με τις πλέον πρόσφατες, κάθε φορά, εκδόσεις τους. Μη τήρηση ιστορικού (ανώνυμη περιήγηση) ή διαγραφή από το ιστορικό των συνδέσμων εκείνων που σχετίζονται με την τηλεργασία, κατά το τέλος της εργασίας.	
4. Διαχωρισμός των αρχείων που περιέχουν προσωπικά δεδομένα, τα οποία σχετίζονται με την εργασία από προσωπικά αρχεία τα οποία τηρεί ο εργαζόμενος στη συσκευή (π.χ. σε σαφώς διακριτούς φακέλους, με κατάλληλη προσδιοριστική ονομασία). Χρήση «εικονικού μηχανήματος» (virtual machine) αποκλειστικά για την παροχή τηλεργασίας, όταν αυτό είναι εφικτό.	
5. Υποστήριξη από τον φορέα διαδικασιών κατάλληλης κρυπτογράφησης αρχείων που περιέχουν προσωπικά δεδομένα, ιδίως όταν τηρούνται σε φορητό/αποσπώμενο μέσο αποθήκευσης (π.χ. usb stick). Ανά περίπτωση, θα πρέπει να εξετάζεται και το ενδεχόμενο κρυπτογράφησης των αρχείων και στην κυρίως συσκευή από την οποία πραγματοποιείται η τηλεργασία (Η/Υ, laptop κτλ.), ιδίως για δεδομένα υψηλού κινδύνου.	
6. Υποστήριξη, από τον φορέα, διαδικασιών λήψης αντιγράφων ασφαλείας για αρχεία με προσωπικά δεδομένα, τα οποία υφίστανται επεξεργασία στο πλαίσιο δραστηριοτήτων τηλεργασίας. Για τα αντίγραφα ασφαλείας πρέπει να τηρούνται μέτρα ανάλογα με όσα περιγράφονται στο σημείο 5.	
7. «Κλείδωμα» της συσκευής από την οποία γίνεται η τηλεργασία (π.χ. προφύλαξη οθόνης, με κωδικό	

απενεργοποίησης) εφόσον μένει, για κάποιο λόγο, χωρίς επιτήρηση.	

Πραγματοποίηση τηλεδιασκέψεων

ΑΠΑΙΤΗΣΗ	ΤΡΟΠΟΣ ΙΚΑΝΟΠΟΙΗΣΗΣ
1. Στην περίπτωση τηλεδιασκέψεων, θα πρέπει να αξιοποιούνται πλατφόρμες που υποστηρίζουν υπηρεσίες ασφαλείας (κρυπτογράφηση). Για παράδειγμα, θα πρέπει να αποφεύγεται λογισμικό τηλεδιάσκεψης το οποίο δεν εξασφαλίζει κρυπτογράφηση από άκρη σε άκρη (end-to-end encryption).	
2. Σε περίπτωση προγραμματισμένης τηλεδιάσκεψης, προστασία του συνδέσμου (link) αυτής (π.χ. όχι δημοσιοποίησή του σε κοινωνικό δίκτυο).	
3. Προσεκτική μελέτη των όρων χρήσης και των όρων προστασίας προσωπικών δεδομένων κατά την επιλογή της λύσης τηλεδιάσκεψης.	