ΠΟΛΙΤΙΚΗ ΠΑΡΟΧΗΣ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΠΡΟΣΒΑΣΗΣ

Πολιτική απομακρυσμένης πρόσβασης και BYOD

1. Σκοπός Σκοπός της παρούσας πολιτικής είναι να θεσπίσει κατευθυντήριες γραμμές για την απομακρυσμένη πρόσβαση στο εσωτερικό δίκτυο του Ινστιτούτου μέσω Εικονικού Ιδιωτικού Δικτύου (VPN) και να ρυθμίσει τη χρήση προσωπικών συσκευών (BYOD) για την πρόσβαση σε ιδρυματικούς πόρους. Η παρούσα πολιτική αποσκοπεί στην ενίσχυση της ασφάλειας, τη διασφάλιση της συμμόρφωσης και την ελαχιστοποίηση των κινδύνων που σχετίζονται με την απομακρυσμένη πρόσβαση και τη χρήση προσωπικών συσκευών.

2. Πεδίο εφαρμογής Η παρούσα πολιτική ισχύει για όλους τους εργαζόμενους, τους εργολάβους, τους προμηθευτές και άλλους τρίτους που χρειάζονται απομακρυσμένη πρόσβαση στο εσωτερικό δίκτυο του οργανισμού. Ισχύει επίσης για όλες τις προσωπικές συσκευές (BYOD) που χρησιμοποιούνται για την πρόσβαση στο δίκτυο, τα συστήματα και τα δεδομένα του οργανισμού.

3. Κατευθυντήριες γραμμές για την απομακρυσμένη πρόσβαση

3.1. Απαιτήσεις πρόσβασης VPN

- Η πρόσβαση VPN πρέπει να ζητείται και να εγκρίνεται από το τμήμα πληροφορικής.
- Στους χρήστες χορηγούνται όνομα χρήστη/κωδικό κωδικός πρόσβασης, τα οποία χρησιμοποιούνται για την πιστοποίηση ταυτότητας πριν από την πρόσβαση στο δίκτυο.
- Η πρόσβαση θα χορηγείται με βάση την αρχή των λιγότερων προνομίων.
- Οι συνδέσεις VPN θα πρέπει να ξεκινούν μόνο από ασφαλείς συσκευές που πληρούν τις απαιτήσεις συμμόρφωσης ασφαλείας.

3.2. Περιορισμοί χρήσης

- Η απομακρυσμένη πρόσβαση πρέπει να χρησιμοποιείται αποκλειστικά για τους επίσημους σκοπούς του Ινστιτούτου.
- Οι χρήστες δεν πρέπει να μοιράζονται τα διαπιστευτήρια VPN με μη εξουσιοδοτημένα άτομα.
- Απαγορεύεται η χρήση δημόσιων ή μη ασφαλών δικτύων για την πρόσβαση στο VPN.
- Οι χρήστες πρέπει να αποσυνδέονται από τις συνόδους VPN όταν δεν χρησιμοποιούνται πλέον.

3.3. Παρακολούθηση και συμμόρφωση

- Όλες οι συνδέσεις VPN θα καταγράφονται και θα παρακολουθούνται για ύποπτη δραστηριότητα.
- Ο οργανισμός διατηρεί το δικαίωμα να ελέγχει τα αρχεία καταγραφής απομακρυσμένης πρόσβασης και να επιβάλλει τη συμμόρφωση με την πολιτική.
- Οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση εντοπιστεί θα έχει ως αποτέλεσμα την άμεση αποσύνδεση και απενεργοποίηση του λογαριασμού.

4. Κατευθυντήριες γραμμές για το BYOD (Bring Your Own Device)

4.1. Απαιτήσεις καταχώρισης και ασφάλειας συσκευών

- Οι εργαζόμενοι πρέπει να καταχωρούν τις προσωπικές τους συσκευές στο τμήμα πληροφορικής πριν αποκτήσουν πρόσβαση σε εταιρικούς πόρους.
- Οι συσκευές πρέπει να διαθέτουν ενημερωμένες επιδιορθώσεις ασφαλείας και ενημερώσεις του λειτουργικού συστήματος.
- Το λογισμικό προστασίας από ιούς και τερματικά σημεία πρέπει να είναι εγκατεστημένο και να ενημερώνεται τακτικά.
- Οι συσκευές πρέπει να είναι κρυπτογραφημένες και να απαιτούν ασφαλή κωδικό πρόσβασης, βιομετρικό έλεγχο ταυτότητας ή ισοδύναμο μηχανισμό ασφαλείας.

4.2. Αποδεκτή χρήση

- Οι προσωπικές συσκευές μπορούν να χρησιμοποιούνται μόνο για καθορισμένους σκοπούς του Ινστιτούτου όταν είναι συνδεδεμένες στο εταιρικό δίκτυο.
- Απαγορεύεται στους χρήστες να κατεβάζουν, να αποθηκεύουν ή να μεταδίδουν ευαίσθητα εταιρικά δεδομένα σε προσωπικές συσκευές, εκτός εάν έχουν λάβει σχετική άδεια.
- Απαγορεύεται αυστηρά η χρήση jailbroken ή rooted συσκευών για εταιρική πρόσβαση.

4.3. Προστασία και πρόληψη απώλειας δεδομένων

- Οι χρήστες πρέπει να αναφέρουν αμέσως στο τμήμα πληροφορικής την απώλεια ή την κλοπή προσωπικών συσκευών.
- Οι χρήστες δεν πρέπει να δημιουργούν αντίγραφα ασφαλείας των εταιρικών δεδομένων σε μη εξουσιοδοτημένους αποθηκευτικούς χώρους στο cloud ή σε προσωπικούς λογαριασμούς.

4.4. Συμμόρφωση και παρακολούθηση

- Το Τμήμα Πληροφορικής διατηρεί το δικαίωμα να ελέγχει τη συμμόρφωση με το BYOD και να επιβάλλει μέτρα ασφαλείας.
- Στις μη συμμορφούμενες συσκευές θα απαγορεύεται η πρόσβαση στο εταιρικό δίκτυο.
- Οι χρήστες που δεν συμμορφώνονται με τις απαιτήσεις ασφαλείας του BYOD ενδέχεται να αντιμετωπίσουν πειθαρχικά μέτρα, συμπεριλαμβανομένης της ανάκλησης των προνομίων πρόσβασης.

5. Αρμοδιότητες

5.1. Ευθύνες των εργαζομένων

- Διασφάλιση ότι οι προσωπικές συσκευές πληρούν όλες τις απαιτήσεις ασφάλειας και συμμόρφωσης.

- Η απομακρυσμένη πρόσβαση και οι προσωπικές συσκευές πρέπει να χρησιμοποιούνται με υπευθυνότητα και σύμφωνα με τις πολιτικές του Ινστιτούτου.
- Αναφέρετε αμέσως τυχόν παραβιάσεις ασφαλείας ή ύποπτες δραστηριότητες στο τμήμα πληροφορικής.

5.2. Αρμοδιότητες του τμήματος πληροφορικής

- Διατήρηση και επιβολή των πολιτικών ασφαλείας του VPN.
- Παροχή κατευθυντήριων γραμμών και υποστήριξης για τους εργαζομένους που χρησιμοποιούν προσωπικές συσκευές για την εργασία τους.
- Παρακολούθηση και διερεύνηση δραστηριοτήτων απομακρυσμένης πρόσβασης για τον εντοπισμό απειλών ασφαλείας.
- Διασφάλιση τακτικών ενημερώσεων και βελτιώσεων των μέτρων ασφαλείας VPN και BYOD.

6. Παραβάσεις της πολιτικής και συνέπειες

- Η παραβίαση της παρούσας πολιτικής μπορεί να οδηγήσει σε πειθαρχικά μέτρα, συμπεριλαμβανομένης της ανάκλησης των προνομίων πρόσβασης, της αναστολής ή της απόλυσης.
- Σε περιπτώσεις παραβίασης δεδομένων, μη εξουσιοδοτημένης πρόσβασης ή κατάχρησης πόρων του Ινστιτούτου ενδέχεται να ληφθούν νομικά μέτρα.

7. Αναθεώρηση και επικαιροποίηση της πολιτικής

- Η παρούσα πολιτική θα επανεξετάζεται ετησίως από τις ομάδες πληροφορικής και ασφάλειας, προκειμένου να διασφαλίζεται η συμμόρφωση με τα εξελισσόμενα πρότυπα ασφαλείας.
- Οι επικαιροποιήσεις της πολιτικής θα κοινοποιούνται σε όλους τους εργαζόμενους και θα απαιτείται επιβεβαίωση της κατανόησης και της συμμόρφωσης.

Με την απομακρυσμένη πρόσβαση στο δίκτυο του οργανισμού ή με τη χρήση προσωπικής συσκευής για εργασιακούς σκοπούς, οι χρήστες αναγνωρίζουν και συμφωνούν να τηρούν την παρούσα πολιτική.