

Πολιτική Εξ Αποστάσεως Πρόσβασης

Σκοπός – Εύρος πολιτικής

Το παρόν έγγραφο αποτελεί Πολιτική του Οργανισμού και αναπόσπαστο τμήμα της Πολιτικής Ασφάλειας. Ορίζει την Πολιτική Εξ Αποστάσεως Πρόσβασης που ακολουθεί ο Οργανισμός σε ότι αφορά την απομακρυσμένη χρήση συστημάτων ΠΕΣ.

Σκοπός της Πολιτικής είναι να προσδιορίσει τις υποχρεώσεις του Οργανισμού και να εκφράσει τη συμμόρφωσή του με το νομικό και κανονιστικό πλαίσιο σχετικά με τη διασφάλιση της προστασίας των διαχειριζόμενων πληροφοριών.

Η ισχύς της παρούσας πολιτικής είναι καθολική, δηλαδή ισχύει για όλο το προσωπικό σε οποιαδήποτε οργανωτική μονάδα του Οργανισμού (Διευθύνσεις, Τμήματα, κ.λπ.) καθώς και για όλους τους συνεργάτες, υπεργολάβους, αναδόχους, συμβούλους, προμηθευτές, πελάτες και γενικότερα για όλα τα φυσικά και νομικά πρόσωπα που χρησιμοποιούν ή / και έρχονται σε επαφή με τις πληροφορίες και τα πληροφοριακά και επικοινωνιακά συστήματα του Οργανισμού.

Η Πολιτική Εξ Αποστάσεως Πρόσβασης καθορίζει τη διαβάθμιση των επιπέδων πρόσβασης και θέτει τις απαιτήσεις για τον έλεγχο πρόσβασης στα ΠΕΣ του Οργανισμού.

Ειδικότερα, περιλαμβάνονται όλα τα δίκτυα, όπως:

- Δίκτυα σταθερών τηλεπικοινωνιών
- IP Networks
- Frame Relay – Data Networks

Περιλαμβάνεται όλος ο εξοπλισμός, όπως:

- Routers, Switches και λοιπός ενεργός εξοπλισμός δικτύωσης
- Τηλεφωνικά κέντρα - PBXs
- Κατανεμητές καλωδιώσεων (κλειδωμένος)

Απαιτήσεις - Υποχρεώσεις

Ο Οργανισμός, εφαρμόζει μέτρα για τον έλεγχο της εξ αποστάσεως πρόσβασης (remote access) στις πληροφοριακές υποδομές του, είτε από το προσωπικό είτε από προσωπικό προμηθευτών ή συνεργάτες του Οργανισμού. Ειδικότερα εφαρμόζονται τα εξής:

- Χρήση κρυπτογραφημένων καναλιών επικοινωνίας για την πρόσβαση σε υπολογιστικούς πόρους του Οργανισμού. Το προσωπικό του Οργανισμού μπορεί να έχει πρόσβαση μόνο μέσω ασφαλών εικονικών δικτύων

(Virtual Private Networks – VPN), χρησιμοποιώντας τα κατάλληλα διαπιστευτήρια (username/ password).

- Επιπρόσθετα, πέρα από τη χρήση διαπιστευτηρίων (username/password), χρησιμοποιείται και η τεχνολογία MFA (Multi-Factor Authentication), με αποστολή ειδοποίησης και αποδοχής στο κινητό τηλέφωνο του χρήστη.
- Κάθε VPN τερματίζει σε δικτυακή συσκευή firewall, όπου εφαρμόζονται κανόνες ελέγχου που επιτρέπουν ή απορρίπτουν την επικοινωνία.
- Η εξ αποστάσεως πρόσβαση των προμηθευτών ή συνεργατών του Οργανισμού στα πληροφοριακά συστήματα για τα οποία έχουν εξουσιοδοτηθεί είναι ελεγχόμενη, διενεργείται για συγκεκριμένους σκοπούς, οι οποίοι είναι εκ των προτέρων γνωστοί στον Οργανισμό και έχουν εγκριθεί ΥΑΠ και οποιονδήποτε άλλο ρόλο απαιτείται ανά περίπτωση (π.χ. Ιδιοκτήτης Πληροφοριών).
- Σε κάθε περίπτωση, για την απομακρυσμένη σύνδεση σε πληροφοριακές υποδομές και πόρους του Οργανισμού, χρησιμοποιούνται μόνο εγκεκριμένες από τον Οργανισμό εφαρμογές.
- Καθένας ο οποίος συνδέεται απομακρυσμένα στις πληροφοριακές υποδομές του Οργανισμού (εργαζόμενος, συνεργάτης, προμηθευτής κ.λπ.) έχει την υποχρέωση να συμμορφώνεται με τα οριζόμενα στην **«Πολιτική Αποδεκτής Χρήσης»** του Οργανισμού.
- Αποτελεί υποχρέωση των εξουσιοδοτημένων για εξ αποστάσεως πρόσβαση χρηστών, να τηρούν αυστηρά προσωπικά τα διαπιστευτήρια πρόσβασης, να μην τα μοιράζονται με τρίτους και να διασφαλίζουν ότι μόνο αυτοί θα συνδέονται απομακρυσμένα σε πληροφοριακές υποδομές και πόρους του Οργανισμού.
- Οι ενέργειες που εκτελούν οι χρήστες οι οποίοι συνδέονται εξ αποστάσεως στις πληροφοριακές υποδομές του Οργανισμού καταγράφονται.

Η διαχείριση των λογαριασμών των χρηστών διενεργείται βάσει των κανόνων που ορίζονται στην **«Πολιτική Ελέγχου Πρόσβασης & Διαχείρισης Χρηστών»**.