

Οδηγίες για τους Υπεύθυνους Διαχειριστές της Υπηρεσίας Τηλε-εργασίας μέσω VPN ΣΥΖΕΥΞΙΣ

Α. Σκοπός του κειμένου

Σκοπός του κειμένου αυτού είναι να ενημερώσει τους Υπεύθυνους Διαχειριστές που ορίστηκαν από τους Δημόσιους Φορείς για την Υπηρεσία Τηλε-εργασίας και να υποστηρίξει τις ενέργειές τους αναφορικά με την χρήση της από τους τελικούς χρήστες. Δεν αποτελεί εγχειρίδιο αντιμετώπισης των πιθανών προβλημάτων που μπορεί να συναντήσει ο Υπεύθυνος Διαχειριστής, αλλά ένα κείμενο που παρέχει μια ξεκάθαρη εικόνα των σημαντικών στοιχείων που πρέπει να γνωρίζει.

Αν και δεν είναι κατεξοχήν τεχνικό κείμενο, ο αναγνώστης με τεχνικές γνώσεις θα μπορέσει να το αξιοποιήσει στον βέλτιστο βαθμό. Υπεύθυνοι Διαχειριστές χωρίς τεχνικές γνώσεις, μπορούν να απευθυνθούν για διευκρινίσεις στο Helpdesk της Υπηρεσίας Τηλε-εργασίας και, ειδικά για τεχνικά θέματα του εσωτερικού τους δικτύου και των υπολογιστών εργασίας, προτείνουμε να απευθυνθούν στον υπεύθυνο για την τεχνική υποστήριξη του φορέα τους.

Β. Τι προσφέρει η υπηρεσία τηλε-εργασίας

Παρέχεται υπηρεσία σύνδεσης στην επιφάνεια εργασίας του υπολογιστή εργασίας (REMOTE DESKTOP). Με αυτή την υπηρεσία ο χρήστης μπορεί μέσω κρυπτογραφημένου καναλιού, να προσπελάσει τα αρχεία στον υπηρεσιακό του υπολογιστή και εν γένει να τον χρησιμοποιήσει όπως όταν βρίσκεται στη εργασία του (π.χ. να έχει πρόσβαση σε εφαρμογές εσωτερικού δικτύου, στο Σύστημα Ηλεκτρονικής Διακίνησης Εγγράφων της υπηρεσίας του κ.λπ.)

Γ. Πως λειτουργεί η υπηρεσία τηλε-εργασίας

Ρόλοι διαχειριστών κάθε υπηρεσίας που θα συμμετέχουν στη δράση:

- Υπεύθυνος Διαχειριστής ο οποίος έχει τεχνικές γνώσεις και έχει δηλωθεί ως πρόσωπο επικοινωνίας για χρήση της υπηρεσίας τηλε-εργασίας.
- υπεύθυνο ΣΥΖΕΥΞΙΣ του Φορέα του ο οποίος θα συνδράμει για το άνοιγμα των απαραίτητων ροών για την επιτυχή σύνδεση.
- i. Ο Υπεύθυνος Διαχειριστής φορέα θα λάβει κωδικούς με διαδικασία που θα του γίνει γνωστή από τη ΓΓΠΣΔΔ, για κάθε χρήστη που περιλαμβάνεται στην αίτησή του.
- ii. Σε συνεργασία με το Helpdesk της υπηρεσίας τηλε-εργασίας, θα κάνει **δοκιμαστική χρήση με έναν από τους κωδικούς**, για να ελέγξει τη λειτουργία της υπηρεσίας και να γίνουν οι απαραίτητες δικτυακές ρυθμίσεις για την λειτουργία όλων των χρηστών.
- iii. Αφού ολοκληρωθεί με επιτυχία η δοκιμαστική χρήση, θα αποστείλει τις οδηγίες εγκατάστασης του VPN και τον κωδικό ατομικά σε κάθε χρήστη του φορέα του.
- iv. Οι τελικοί χρήστες θα επικοινωνούν με τον Υπεύθυνο Διαχειριστή του φορέα τους για τυχόν προβλήματα ή ερωτήσεις σχετικές με την υπηρεσία. **Για κάθε φορέα η**

επικοινωνία με το Helpdesk της υπηρεσίας τηλε-εργασίας θα πραγματοποιείται αποκλειστικά μέσω του Υπεύθυνου Διαχειριστή του φορέα.

Για τους ανωτέρω λόγους θεωρούμε σημαντικό **ο Υπεύθυνος Διαχειριστής του φορέα να έχει τεχνικές γνώσεις.**

Δ. Helpdesk Υπηρεσίας τηλε-εργασίας

Το Helpdesk της υπηρεσίας είναι εγκατεστημένο στην ΓΓ Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (ΓΓΠΣΔΔ) και μπορεί να:

- βοηθήσει σε διαδικαστικά και λειτουργικά θέματα σχετικά με την ενεργοποίηση της υπηρεσίας τηλε-εργασίας
- κατευθύνει σε τεχνικά θέματα που σχετίζονται με το ΣΥΖΕΥΞΙΣ.

Το Helpdesk της ΓΓΠΣΔΔ δεν μπορεί να επιλύσει προβλήματα που σχετίζονται με το εσωτερικό δίκτυο των φορέων ή με τους οικιακούς υπολογιστές των τελικών χρηστών. Σε αυτές τις περιπτώσεις, ο Υπεύθυνος Διαχειριστής του Φορέα επικοινωνεί μέσω email με τη ΓΓΠΣΔΔ (vpn-dhmosio@gsis.gr). Εξειδικευμένος τεχνικός προσπαθεί να βοηθήσει συμβουλευτικά με οδηγίες. Οι οδηγίες που παρέχονται στις επόμενες ενότητες του παρόντος αναλύουν σε ένα ικανοποιητικό βαθμό τις τεχνικές λεπτομέρειες της δράσης.

Η επικοινωνία των φορέων με το Helpdesk γίνεται **αποκλειστικά μέσω των Υπεύθυνων Διαχειριστών** που έχουν οριστεί, με τους παρακάτω τρόπους:

1. Τηλεφωνικά στον αριθμό **213.13.33.093** (επιλογή 2: Υπηρεσία τηλε-εργασίας)
2. Μέσω email στη διεύθυνση vpn-dhmosio@gsis.gr.

Ε. Προϋποθέσεις για χρήση τηλε-εργασίας

ii. Υπολογιστές Εργασίας (που βρίσκονται στο γραφείο του υπαλλήλου)

- Στην περίπτωση υπολογιστών γραφείου με λειτουργικό σύστημα Windows, η χρήση του Remote Desktop (server) δεν υποστηρίζεται εγγενώς στις Home εκδόσεις. Στις περιπτώσεις αυτές η προσπάθεια σύνδεσης από απομακρυσμένο Η/Υ σε Η/Υ γραφείου με windows home Edition δεν επιτρέπει τη χρήση της υπηρεσίας τηλε-εργασίας.
- Οι υπολογιστές εργασίας (γραφείου) στους οποίους θα συνδεθούν χρήστες με Remote Desktop, θα πρέπει να είναι συνδεδεμένοι σε τοπικό δίκτυο και **να έχουν ρυθμιστεί με IP διεύθυνση ΣΥΖΕΥΞΙΣ**. Σε περίπτωση που ενώ η υπηρεσία είναι στο ΣΥΖΕΥΞΙΣ, οι Η/Υ έχουν private IPs της μορφής 192.X.X.X ή 172.X.X.X, απαιτούνται τεχνικές ρυθμίσεις στο εσωτερικό δίκτυο ώστε να αντιστοιχιστεί κάθε IP των υπολογιστών με μία IP ΣΥΖΕΥΞΙΣ από το LAN που έχει δοθεί στο φορέα (π.χ. με static NAT)
- Αν οι IP δίνονται στους υπολογιστές με DHCP, λάβετε υπόψη ότι είναι προτιμότερο να αποδοθούν στατικές IP, διαφορετικά, αν ο υπολογιστής κλείσει, η IP του μπορεί να αλλάξει και ο τελικός χρήστης να μην μπορεί να συνδεθεί από το σπίτι αν δεν γνωρίζει την νέα IP. Ωστόσο αν ο Η/Υ του γραφείου παραμείνει μονιμα ανοιχτός έχει

ένα συγκεκριμένο ip. Αν γνωστοποιηθεί αυτό το ip στο χρήστη, εκείνος μπορεί να πραγματοποιήσει απομακρυσμένη πρόσβαση στο Η/Υ του γραφείου του.

- Οι υπολογιστές εργασίας προτείνουμε να έχουν απενεργοποιημένη την αναστολή λειτουργίας (sleep mode, / control panel, power setting), διαφορετικά ίσως να μην είναι δυνατή η απομακρυσμένη σύνδεση σε αυτά.
- Οι υπολογιστές εργασίας θα πρέπει να έχουν **ενεργοποιημένη την υπηρεσία απομακρυσμένης επιφάνειας εργασίας**.
- Κάθε υπολογιστής εργασίας θα πρέπει **να επιτρέπει**, με σχετική ρύθμιση, την **απομακρυσμένη σύνδεση του συγκεκριμένου χρήστη** σε αυτόν (remote desktop users), γιατί ανάλογα με τον τύπο του (απλός ή διαχειριστής) μπορεί να μην επιτρέπεται. Σε περίπτωση που δεν επιτρέπεται ο Υπεύθυνος Διαχειριστής δύναται να κάνει τις απαραίτητες ρυθμίσεις τους Η/Υ της εργασίας.
- Το firewall των Windows ή άλλο αντίστοιχο λογισμικό που ρυθμίζει την δικτυακή κίνηση στον υπολογιστή θα πρέπει να ρυθμιστεί κατάλληλα, ώστε να επιτρέπει την εισερχόμενη κίνηση RDP από τις IP του vrn.
- Κατά τη σύνδεση από τον οικιακό υπολογιστή στον υπολογιστή εργασίας, θα ζητηθεί από το Remote Desktop, username και password. Το username θα πρέπει να γράφεται με την μορφή ΌνομαΥπολογιστή\username ή Τομέας\username, ανάλογα με τον τρόπο που συνδέεται ο χρήστης στην εργασία του (σύνδεση σε τομέα [domain] ή τοπική σύνδεση).

iii. Δικτυακός Εξοπλισμός (router, firewall, switches)

- Ενδέχεται να χρειαστούν παραμετροποίηση τυχόν δικτυακές συσκευές (firewall, switches, router) του εσωτερικού δικτύου του φορέα, προκειμένου να επιτραπεί η πρόσβαση στο destination port για το πρωτόκολλο RDP από τις IP των χρηστών VPN. Οι ρυθμίσεις αυτές αφορούν:
 - Το εσωτερικό δίκτυο των φορέων, οι οποίες πρέπει να γίνουν με μέριμνα του Τεχνικού Υπεύθυνου της υπηρεσίας.
 - Οι IP από τις οποίες θα απαιτηθεί πρόσβαση, αναφέρονται στο email που στάλθηκε στον Υπεύθυνο Διαχειριστή του φορέα σχετικά με την ενεργοποίηση των λογαριασμών vrn των τελικών χρηστών. Σε κάθε περίπτωση, μπορεί να ζητηθούν και από το Helpdesk της ΓΓΠΣΔΔ.
- Για τον ίδιο λόγο ενδέχεται να απαιτηθούν ρυθμίσεις στην περιμετρική ασφάλεια του router ΣΥΖΕΥΞΙΣ. Γι' αυτό θα πρέπει ο ορισμένος Υπεύθυνος Διαχειριστής του φορέα για την υπηρεσία VPN, **να επικοινωνήσει με τον τεχνικό υπεύθυνο ΣΥΖΕΥΞΙΣ** ο οποίος έχει την αρμοδιότητα υποβολής αιτημάτων άρσης της περιμετρικής ασφάλειας στο Helpdesk του ΣΥΖΕΥΞΙΣ.

Για διευκόλυνση των φορέων προτείνουμε, ο Υπεύθυνος Διαχειριστής, με την έναρξη της δοκιμαστικής χρήσης της υπηρεσίας τηλε-εργασίας, να ενημερώσει τον Υπεύθυνο ΣΥΖΕΥΞΙΣ για τις απαιτούμενες ρυθμίσεις στον router ΣΥΖΕΥΞΙΣ. Κατ' εξαίρεση της τυπικής διαδικασίας άρσης περιμετρικής ασφάλειας του router ΣΥΖΕΥΞΙΣ, ο Υπεύθυνος ΣΥΖΕΥΞΙΣ μπορεί να απευθυνθεί στο Helpdesk της υπηρεσίας τηλε-εργασίας υποβάλλοντας αίτημα, ώστε να επιτραπεί η εισερχόμενη δικτυακή κίνηση RDP από τις IP των VPN χρηστών προς τις LAN IP των υπολογιστών εργασίας του φορέα. Το Helpdesk Τηλε-εργασίας, θα εγκρίνει και θα προωθήσει με προτεραιότητα το αίτημα στο Helpdesk ΣΥΖΕΥΞΙΣ.

ΣΤ. Σημαντικές ενέργειες του Διαχειριστή

Ανάλογα με την τεχνική εγκατάσταση σε κάθε φορέα, ενδέχεται να απαιτηθούν όλες ή ορισμένες μόνο από τις ανωτέρω ενέργειες. Κάποιες από αυτές, όμως, είναι ιδιαίτερα σημαντικό να εξασφαλισθούν εξ αρχής για την ταχύτερη και αποτελεσματικότερη χρήση της υπηρεσίας τηλε-εργασίας. Συνοπτικά:

1. Ο Υπεύθυνος Διαχειριστής του φορέα να έχει τεχνικές γνώσεις ή άμεση πρόσβαση σε τεχνική ομάδα που μπορεί να ρυθμίσει τον εσωτερικό δικτυακό εξοπλισμό και τους υπολογιστές εργασίας εάν χρειαστεί.
2. Με την λήψη των κωδικών των τελικών χρηστών και πριν την αποστολή τους σε αυτούς, ο Υπεύθυνος Διαχειριστής διενεργεί δοκιμαστική σύνδεση με τους δικούς του κωδικούς και επικοινωνεί με το Helpdesk της υπηρεσίας τηλε-εργασίας για τυχόν προβλήματα ή απορίες, προκειμένου να γίνουν οι απαραίτητες ρυθμίσεις για την ενεργοποίησή της.
3. Εάν χρειάζεται αίτημα άρσης της περιμετρικής ασφάλειας στον router ΣΥΖΕΥΞΙΣ από τον Τεχνικό Υπεύθυνο ΣΥΖΕΥΞΙΣ του φορέα, προτείνεται να ακολουθήσετε την οδηγία που αναγράφεται στο πράσινο πλαίσιο παραπάνω.
4. Μετά την επιτυχημένη δοκιμαστική σύνδεση ο Υπεύθυνος Διαχειριστής του φορέα μπορεί να αποστείλει στους τελικούς χρήστες τις πληροφορίες που χρειάζονται για εργαστούν απομακρυσμένα. Οι τελικοί χρήστες επικοινωνούν με τον Υπεύθυνο Διαχειριστή του φορέα τους για τυχόν υποστήριξη κατά την ενεργοποίηση της τηλε-εργασίας. Το Helpdesk της υπηρεσίας τηλε-εργασίας παρέχει υποστήριξη στους φορείς μόνο μέσω του Υπεύθυνου Διαχειριστή τους.
5. Ιδιαίτερη μέριμνα θα πρέπει να δοθεί στην αποστολή των κωδικών η οποία δεν πρέπει να γίνει μαζικά, αλλά ατομικά σε κάθε χρήστη της υπηρεσίας, ώστε κάθε χρήστης να μάθει μόνο τον δικό του κωδικό και όχι άλλων χρηστών.
6. Για αλλαγή του κωδικού από τον χρήστη, θα σας σταλούν εκ νέου οδηγίες τις επόμενες ημέρες. Εάν ένας χρήστης ξεχάσει τον κωδικό του, θα πρέπει να ενημερώσει τον Υπεύθυνο Διαχειριστή του φορέα του και ο διαχειριστής να επικοινωνήσει με το Helpdesk της υπηρεσίας.

Ζ. Σημαντικές ενέργειες των τελικών χρηστών

Για να αξιοποιηθεί η VPN σύνδεση αποκλειστικά για τον προβλεπόμενο σκοπό, με ασφάλεια και να ελαχιστοποιηθεί η πιθανότητα να τεθεί σε κίνδυνο το δίκτυο εργασίας, θα πρέπει οι Υπεύθυνοι Διαχειριστές των φορέων να εξασφαλίσουν για τους τελικούς χρήστες του φορέα τους, στο μέτρο του δυνατού, τα ακόλουθα:

1. Ο τελικός χρήστης είναι στέλεχος του φορέα ή εξουσιοδοτημένος συνεργάτης με άδεια να εργαστεί εξ' αποστάσεως για λογαριασμό του φορέα.
2. Είναι απαραίτητη η απομακρυσμένη πρόσβαση του τελικού χρήστη στην υπηρεσία.
3. Ο τελικός χρήστης θα κάνει χρήση της υπηρεσίας καθαρά και μόνο για υπηρεσιακούς σκοπούς.
4. Ο οικιακός υπολογιστής που θα χρησιμοποιηθεί να διαθέτει σύνδεση στο Διαδίκτυο, λειτουργικό σύστημα ενημερωμένο με τις τελευταίες εκδόσεις

ασφαλείας, καθώς και εγκατεστημένο, ενημερωμένο και ενεργό πρόγραμμα προστασίας από ιούς.

5. Ο οικιακός υπολογιστής είναι επιθυμητό να έχει ενεργοποιημένο το «τείχος προστασίας» (firewall) των windows.
6. Ο οικιακός υπολογιστής δεν πρέπει να εκτελεί εφαρμογές κατά την διάρκεια μιας απομακρυσμένης σύνδεσης (π.χ. Internet browsing, σύνδεση σε κοινωνικά δίκτυα, μεταφόρτωση ταινιών/αρχείων κ.λπ.). Γι' αυτό και με την σύνδεση στο VPN διακόπτεται κάθε άλλη επικοινωνία με το Internet για τον οικιακό υπολογιστή. Με την αποσύνδεση από το VPN η δικτυακή δραστηριότητα του οικιακού υπολογιστή επανέρχεται σε κανονική λειτουργία.
7. Δεν θα πρέπει να ανακοινωθεί ή να δοθεί κανένα από τα στοιχεία πρόσβασης στο VPN, σε οποιονδήποτε.

Θα πρέπει οι Υπεύθυνοι Διαχειριστές των φορέων να επισημάνουν στους τελικούς χρήστες που χρησιμοποιούν τον οικιακό τους υπολογιστή για να συνδεθούν απομακρυσμένα με τον υπολογιστή εργασίας, πως είναι υπεύθυνοι για την ασφάλεια του υπολογιστή που χρησιμοποιούν και ότι πρέπει να λάβουν όλα τα μέτρα που εγγυώνται την ασφαλή απομακρυσμένη εργασία, σύμφωνα με τις υποδείξεις τους.