ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ **Νοέμβριος 2022**
ΠΕΡΙΦΕΡΕΙΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΓΕΝ. Δ/ΝΣΗ ΕΣΩΤΕΡΙΚΗΣ ΛΕΙΤΟΥΡΓΙΑΣ
Δ/ΝΣΗ ΔΙΑΦΑΝΕΙΑΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΠΟΛΙΤΙΚΗ ΔΕΟΝΤΟΛΟΓΙΑΣ
ΟΡΘΗΣ ΚΑΙ ΑΣΦΑΛΟΥΣ ΧΡΗΣΗΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΤΗΣ ΠΕΡΙΦΕΡΕΙΑΣ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

Η Πολιτική αυτή αφορά τη χρήση των Πληροφοριακών Συστημάτων και Πληροφορικής Τεχνολογίας **(εφεξής Π.Σ.&Π.Τ.)** της Περιφέρειας Δυτικής Ελλάδας (Π.Δ.Ε.) όπως την πρόσβαση στα υπολογιστικά συστήματα και τον ψηφιακό εξοπλισμό, τους προσωπικούς και φορητούς Η/Υ, τους εξυπηρετητές, εκτυπωτές, σαρωτές, το λογισμικό, τις υπηρεσίες και εφαρμογές δικτύου και διαδικτύου, τις βάσεις δεδομένων και λοιπά πληροφοριακά συστήματα, τις ηλεκτρονικές σελίδες, το τηλεφωνικό δίκτυο και τις συσκευές αυτού, το υπηρεσιακό ηλεκτρονικό ταχυδρομείο και την πρόσβαση στο Διαδίκτυο.

Η Πολιτική αφορά το μόνιμο, επί συμβάσει, (ΙΔΟΧ, προγραμμάτων ωφελουμένων ορισμένου χρόνου ΟΑΕΔ κ.τ.λ.), ασκούμενο (πρακτικής άσκησης σπουδαστών-φοιτητών) προσωπικό και εξωτερικούς χρήστες **(εφεξής υπόχρεοι)** και εφαρμόζεται:

- σε εξοπλισμό και συστήματα που αποτελούν ιδιοκτησία της Π.Δ.Ε. και του Δημοσίου με την ευρύτερη έννοια,
- σε προσωπικό εξοπλισμό που χρησιμοποιεί τη δικτύωση και τους πόρους των πληροφοριακών συστημάτων της Π.Δ.Ε,
- σε υπηρεσίες και συστήματα που παρέχονται και διευθύνονται από τη Δ/νση Διαφάνειας & Ηλ. Διακυβέρνησης της Π.Δ.Ε,
- σε υπηρεσίες που είναι εγκατεστημένες στον προσωπικό εξοπλισμό υπαλλήλων που συνδέονται προσωρινά ή μόνιμα στο δίκτυο της Π.Δ.Ε,
- σε οποιαδήποτε άλλα συστήματα τα οποία αποκτούν, εξουσιοδοτημένη ή μη, σύνδεση & πρόσβαση στο δίκτυο της Π.Δ.Ε. και χρησιμοποιούν διευθύνσεις Διαδικτύου που έχουν παραχωρηθεί στην Π.Δ.Ε,
- σε ενέργειες που ξεκινούν από υπολογιστικά συστήματα ή κινητές συσκευές που διατηρούνται ή χρησιμοποιούνται, εκτός Π.Δ.Ε και των γραμμών ΣΥΖΕΥΞΙΣ, από υπαλλήλους της Π.Δ.Ε. που συνδέονται εξ αποστάσεως με το Δίκτυο της Π.Δ.Ε.

Ειδικότερα, η Πολιτική έχει την ίδια ισχύ σε ενέργειες υποχρέων που συνδέονται στα πληροφοριακά συστήματα μέσω ιδιωτικών συσκευών και προσωπικού εξοπλισμού και χρησιμοποιούν την υπηρεσία πρόσβασης στο δίκτυό της.
(Τέτοιος προσωπικός εξοπλισμός, ο οποίος προσαρτάται, συνδέεται και χρησιμοποιεί πόρους της Π.Δ.Ε., υπόκειται στο ίδιο καθεστώς με τον εξοπλισμό της Π.Δ.Ε.)

Κάθε χρήστης των Πληροφοριακών Συστημάτων και Πληροφορικής Τεχνολογίας (Π.Σ.&Π.Τ.) της Π.Δ.Ε., θα πρέπει να συνεισφέρει στην ασφάλεια των πληροφοριών και των υποδομών στις οποίες έχει πρόσβαση, με την ορθή χρήση των πόρων τους και την τήρηση των θεμελιωδών κανόνων ορθής/ασφαλούς χρήσης και δεοντολογίας. Αρμόδια πρόσωπα για τη

μετάδοση κάθε αναφοράς για την τήρηση ή μη των κανόνων αυτών από το προσωπικό των Υπηρεσιών της Π.Δ.Ε., είναι οι Προϊστάμενοι των Διευθύνσεων και για τα Γραφεία Αντιπεριφερειαρχών, Προέδρων Συλλογικών Οργάνων και Επιτροπών οι Πρόεδροι αυτών. Αρμόδια Υπηρεσία λήψης των αιτημάτων είναι η Διεύθυνση Διαφάνειας και Ηλεκτρονικής Διακυβέρνησης (Δ.Δ.Η.Δ.), η οποία επιλαμβάνεται για κάθε θέμα που αντιβαίνει στην πολιτική δεοντολογίας και ορθής χρήσης των Π.Σ.&Π.Τ της Π.Δ.Ε.

Η Πολιτική αυτή διέπεται από τις ισχύουσες διατάξεις οργάνωσης και λειτουργίας του Δημοσίου, της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό Cert), του κανονισμού Επικοινωνίας Δημοσίων Υπηρεσιών (ΚΕΔΥ), του Ν.3528/2007 (ΦΕΚ Α΄ 26 - Υπαλληλικός Κώδικας όπως ισχύει), του Ν.4057/2012 (Πειθαρχικό Δίκαιο Δημοσίων Πολιτικών Διοικητικών Υπαλλήλων και Υπαλλήλων Νομικών Προσώπων Δημοσίου Δικαίου) σε συνδυασμό με τις διατάξεις του άρθρου 6 παρ κγ΄ του Ν. 4325/2015 όπως ισχύει μετά την αντικατάσταση του άρθρου 107 του Ν.3528/2007, όπου στα πειθαρχικά παραπτώματα έχει ενταχθεί ***«η φθορά λόγω ασυνήθιστης χρήσης, η εγκατάλειψη ή η παράνομη χρήση πράγματος το οποίο ανήκει στην υπηρεσία»*** που τιμωρείται σύμφωνα με τις διατάξεις του άρθρου 4 (πειθαρχικές ποινές) του ίδιου Νόμου.

Όποιος εμπίπτει στους υπόχρεους εφαρμογής της Πολιτικής Δεοντολογίας / Ορθής Χρήσης Π.Σ.&Π.Τ. στην Π.Δ.Ε. θα πρέπει:

Α. ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

1. Να τηρεί εχεμύθεια για θέματα που χαρακτηρίζονται απόρρητα από τις κείμενες διατάξεις,[1] ή όταν αυτό επιβάλλεται από την κοινή πείρα και λογική, για γεγονότα ή πληροφορίες των οποίων λαμβάνει γνώση ή επεξεργάζεται κατά την εκτέλεση των καθηκόντων του.
2. Να περιορίζεται μόνο στην πρόσβαση και εν γένει επεξεργασία των πληροφοριών που είναι απαραίτητες για την εκτέλεση των καθηκόντων του.
3. Να λαμβάνει μέριμνα για την όσο το δυνατόν ευκρινή ταξινόμηση των ψηφιακών υπηρεσιακών φακέλων και εγγράφων που αποθηκεύει στον προσωπικό του Η/Υ, γνωρίζοντας ότι το υπηρεσιακό αυτό υλικό, ανήκει στο Δημόσιο και οφείλει να το παραδώσει εξ ολοκλήρου σε κάθε περίπτωση αποχώρησής του (μόνιμης ή προσωρινής).
4. Να γνωρίζει ότι οποιαδήποτε ενέργεια (δηλ. καταχώρηση, μεταβολή, διαγραφή, εμφάνιση ή εκτύπωση στοιχείων) που πραγματοποιείται στα Π.Σ., δύναται να καταγράφεται και μπορεί να αποδοθεί στον υπάλληλο που την πραγματοποίησε, όπως περιγράφεται στην Πολιτική Προστασίας Προσωπικών Δεδομένων των Εργαζομένων που έχει καταρτίσει η Π.Δ.Ε.

Β. ΟΡΘΗ ΧΡΗΣΗ

1. Να χρησιμοποιεί μόνο κατάλληλα αδειοδοτημένο λογισμικό της Π.Δ.Ε., και εν γένει, να σέβεται τα πνευματικά δικαιώματα και την ιδιοκτησία.
2. Να μην επιτρέπει τη χρήση του εξοπλισμού που του έχει διατεθεί σε μη εξουσιοδοτημένα πρόσωπα (επισκέπτες κ.ά).
3. Να μην εγκαθιστά/συνδέει εξοπλισμό (δρομολογητές, μεταγωγείς, ασύρματα σημεία πρόσβασης, εξωτερικούς σκληρούς δίσκους και φορητές συσκευές αποθήκευσης

[1] *Ν. 4624/2019 για την εφαρμογή στην Ελληνική Επικράτεια του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΕΕ) 2016/679 «ΓΚΠΔ», & Ν. 3471/06 για την Προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών.*

δεδομένων όπως CD και USBsticks, Η/Υ, εξυπηρετητές, κ.α.) στα δίκτυα της Π.Δ.Ε. και να ενημερώνει για τυχόν τέτοιες ανάγκες την Δ.Δ.Η.Δ. ώστε η όποια παρέμβαση να γίνεται από εξουσιοδοτημένο και μόνο προσωπικό.

4. Να μην εγκαθιστά λογισμικό στους Η/Υ της Υπηρεσίας, και να ενημερώνει για τυχόν τέτοια ανάγκη τη Δ.Δ.Η.Δ. ώστε η όποια παρέμβαση να γίνεται από εξουσιοδοτημένο και μόνο προσωπικό της ΠΔΕ.
5. Να μην αποθηκεύει μη υπηρεσιακά αρχεία (λ.χ. φωτογραφίες, βίντεο, αρχεία μουσικής) στο δίκτυο και τους πόρους της Π.Δ.Ε., ειδικά δε, στους κοινόχρηστους υπηρεσιακούς πόρους που εξυπηρετούν τις Υπηρεσίες της Π.Δ.Ε.
6. Να μην προβαίνει σε: **α)** καθ' οιονδήποτε τρόπο εκμετάλλευση πιθανών κενών ασφάλειας του ηλεκτρονικού εξοπλισμού (τηλεπικοινωνιακού, διαδικτύου κ.τ.λ) στο οποίο του έχει (ή όχι) επιτραπεί η πρόσβαση, **β)** προσβολή ή κακή χρήση των συστημάτων, υπηρεσιών και εφαρμογών της Π.Δ.Ε., **γ)** διατάραξη της ομαλής λειτουργίας των δικτύων και υπηρεσιών της Π.Δ.Ε. και **δ)** εκτέλεση οποιουδήποτε κακόβουλου λογισμικού που δύναται να θέσει σε κίνδυνο ή να υποβαθμίσει το επίπεδο ασφάλειας των Π.Σ. της Π.Δ.Ε.
7. Σε περίπτωση υποψιών, ή διαπίστωσης συμβάντος ανασφάλειας, ή τρωτότητας, ή διάπραξης αδικήματος που εμπλέκει τα συστήματα Πληροφορικής Τεχνολογίας, θα πρέπει να ειδοποιεί άμεσα τον Προϊστάμενο της Υπηρεσίας στην οποία υπηρετεί παρέχοντας όλες τις σχετικές πληροφορίες, και ο τελευταίος έχει την υποχρέωση να ενημερώσει άμεσα τη Δ.Δ.Η.Δ.
8. Να μην επιδιώκει την μη εξουσιοδοτημένη πρόσβαση στον προσωπικό εξοπλισμό, λογαριασμό ή ιδιωτική επικοινωνία των μελών της Π.Δ.Ε. Σε περίπτωση που οποιοσδήποτε αποκτήσει τέτοια πρόσβαση, οφείλει να την τερματίσει αμέσως και να προβεί σε άμεση ειδοποίηση του επηρεαζόμενου προσώπου για το συμβάν.
9. Να μην επιδιώκει την μη εξουσιοδοτημένη πρόσβαση στα ηλεκτρονικά αρχεία του προσωπικού της Π.Δ.Ε. Απαγορεύεται ιδίως οποιαδήποτε ενέργεια για την μη εξουσιοδοτημένη αναζήτηση, ανάκτηση, πρόσβαση, αντιγραφή, χρήση, τροποποίηση ή διαγραφή ηλεκτρονικών κειμένων, αρχείων, κωδικών, εικόνων, φίλμ, ηχητικών και οπτικών αρχείων και προγραμμάτων.

Γ. ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ / ΗΛΕΚΤΡΟΝΙΚΟΥ ΥΠΗΡΕΣΙΑΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

1. Να μην χρησιμοποιεί τους πόρους της Π.Δ.Ε. για προσωπικούς σκοπούς, ειδικότερα όπως περιγράφεται στις επόμενες παραγράφους.
2. Να μην κάνει χρήση του διαδικτύου και του υπηρεσιακού (e-mail) ηλεκτρονικού ταχυδρομείου με τρόπο που αντιβαίνει τον υπηρεσιακό ρόλο του και προσβάλλει το κύρος του Δημοσίου και της Π.Δ.Ε.
3. Να χρησιμοποιεί αποκλειστικά το δικό του υπολογιστικό σύστημα στο οποίο έχει εγκατασταθεί ο προσωπικός λογαριασμός ηλεκτρονικού ταχυδρομείου για τη διακίνηση ηλεκτρονικών μηνυμάτων (emails) , να μην επιτρέπει τη χρήση του λογαριασμού αυτού από άλλους, όπως και να μην προβαίνει στη μη εξουσιοδοτημένη χρήση αντίστοιχου λογαριασμού σε άλλο υπολογιστικό σύστημα με οποιοδήποτε σκοπό (λ.χ. εξυπηρέτηση υπηρεσιακού έργου).
4. Να μη διακινεί μηνύματα με παράνομο ή άσεμνο περιεχόμενο, ή με κακόβουλο/ιομορφικό λογισμικό.
5. Να μην αποστέλλει σε άλλους χρήστες, ανεπιθύμητα ηλεκτρονικά μηνύματα (unsolicitedmails ή junkmails) ή άλλου διαφημιστικού ή προωθητικού περιεχομένου (spams).

6. Να μην αποστέλλει μη υπηρεσιακά δεδομένα/αρχεία μέσω του υπηρεσιακού e-mail, που εμπίπτουν στην ιδιωτική ζωή ή αφορούν άσκηση ιδιωτικού έργου με αμοιβή (ή μη) ανεξάρτητα αν έχει λάβει τη σχετική υπηρεσιακή άδεια, καθόσον αυτό (το έργο) αφορά εργασία που δεν σχετίζεται με τα υπηρεσιακά καθήκοντα.
7. Να μην αποστέλλει υπηρεσιακά δεδομένα/αρχεία μέσω μη υπηρεσιακού ηλεκτρονικού ταχυδρομείου (ελεύθερου provider).
8. Να μην διακινεί πληροφορίες εμπιστευτικές/απόρρητες, ή και μη εμπιστευτικές, προσωπικά δεδομένα πολιτών μέσω ηλεκτρονικού ταχυδρομείου, ή του διαδικτύου. Εφόσον αυτό είναι υποχρεωτικό για λόγους υπηρεσιακούς, θα πρέπει να προβεί στη λήψη μέτρων που καθιστούν ασφαλή τη μετάδοση της πληροφορίας (π.χ. κρυπτογράφηση) σε συνεννόηση με τον υπηρεσιακό αποδέκτη (Υπουργείο, Ο.Τ.Α., Ν.Π.Δ.Δ.). Ρητά απαγορεύεται η αποστολή των παραπάνω πληροφοριών ή αρχείων που εμπεριέχουν τέτοιες πληροφορίες σε προσωπικές διευθύνσεις ηλεκτρονικού ταχυδρομείου υπαλλήλων με το πρόσχημα της εξ αποστάσεως εργασίας (τηλεργασίας). Για την σωστή και λειτουργική εξ αποστάσεως εργασία των υπαλλήλων θα παραχωρείται πρόσβαση στα συστήματα της Π.Δ.Ε. από την Δ.Δ.Η.Δ., με την χρήση των κατάλληλων μέτρων προστασίας (λ.χ. μέσω VPN).
9. Να είναι ιδιαίτερα προσεκτικός στο άνοιγμα ή τη διαχείριση (προώθηση) μηνυμάτων στα οποία περιέχονται συνημμένα αρχεία και σύνδεσμοι (links), το περιεχόμενο των οποίων δεν είναι εύλογο ή ο αποστολέας είναι άγνωστος.
10. Όταν προωθεί μήνυμα ηλεκτρονικού ταχυδρομείου σε πολλούς παραλήπτες να χρησιμοποιεί την κρυφή/ιδιαίτερη κοινοποίηση (BCC).
11. Να χρησιμοποιεί ενημερωμένο πρόγραμμα πλοήγησης και ηλεκτρονικού ταχυδρομείου και να γνωστοποιεί άμεσα τη Δ.Δ.Η.Δ. σε περίπτωση που τα προγράμματα αυτά δεν είναι ενημερωμένα.
12. Να μην δίνει τα υπηρεσιακά και προσωπικά του στοιχεία παρά μόνο σε ιστοτόπους που είναι έμπιστοι και εγκεκριμένοι από την Π.Δ.Ε.

Δ. ΔΙΑΧΕΙΡΙΣΗ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

1. Ο υπάλληλος που έχει δικαιώματα απλού χρήστη (user) στον υπηρεσιακό, προσωπικό του Η/Υ, θα πρέπει να εισέρχεται με τους κωδικούς που του έχουν παρασχεθεί για αυτό το επίπεδο χρήσης του συστήματός του.
2. Ο υπάλληλος που δεν έχει δικαιώματα διαχειριστή συστήματος (administrator) δεν πρέπει να εισέρχεται ως διαχειριστής, μεταβάλλοντας τις ρυθμίσεις του Η/Υ, προσθαφαιρώντας λογισμικό, νόμιμο (αγορασμένο με άδεια χρήσης) ή παράνομο (κλεψίτυπο, «σπασμένο» κ.τ.λ). Σε περίπτωση που γνωρίζει τους κωδικούς εισόδου administrator θα πρέπει να γνωρίσει τούτο στον Προϊστάμενο της Διεύθυνσης που υπηρετεί.
3. Να τηρεί μυστικά τα στοιχεία των προσωπικών λογαριασμών του (όνομα χρήστη, κωδικός) για κάθε ψηφιακή υπηρεσία στην οποία έχει εγγραφεί με δικαιώματα πρόσβασης ή ανάρτησης (π.χ. πρόγραμμα «ΔΙΑΥΓΕΙΑ». e-procurement.gov.gr, opendata.gov.gr, site Π.Δ.Ε. κ.τ.λ.) και να ειδοποιεί άμεσα τον Προϊστάμενο της Διεύθυνσης που υπηρετεί για τυχόν διαρροή τους. Στη συνέχεια, πρέπει να ανακοινώνεται εγγράφως στη Δ.Δ.Η.Δ. η απώλεια του κωδικού πρόσβασης ώστε αυτός να απενεργοποιείται και να χορηγείται νέος.
4. Να μην κοινοποιεί σε κανέναν τρίτο με κανένα μέσο, προφορικό, γραπτό, ψηφιακό (τηλεφωνικά, μέσω e-mail κ.τ.λ.) τους προσωπικούς κωδικούς πρόσβασής του στα

προαναφερόμενα συστήματα. Οι κωδικοί πρόσβασης θα πρέπει να μην έχουν αποθηκευθεί σε σημεία όπου μπορούν να αποκαλυφθούν (π.χ. σε εκτεθειμένα χαρτιά ή ψηφιακά αρχεία εύκολα προσβάσιμα όπως αρχεία σε μορφή απλού κειμένου ή απροστάτευτου word).

5. Να μην παραχωρεί τους προσωπικούς κωδικούς πρόσβασης Π.Σ.&Π.Τ. σε άλλα πρόσωπα (π.χ. συναδέλφους υπαλλήλους ή σπουδαστές που πραγματοποιούν πρακτική άσκηση) προκειμένου να πραγματοποιήσουν υπηρεσιακό έργο επ' ονόματί του. Σε περίπτωση που προχωρήσει σε μία τέτοια ενέργεια, οποιαδήποτε κίνηση πραγματοποιηθεί με τους κωδικούς αυτούς θεωρείται ότι υλοποιήθηκε από αυτόν.
6. Να λαμβάνει μέριμνα ώστε να αλλάζει περιοδικά τους κωδικούς πρόσβασής του σε κάθε ψηφιακό σύστημα που έχει πρόσβαση, να αποφεύγει την χρήση του ίδιου κωδικού σε όλα τα συστήματα και να μην τους καταγράφει, αλλά να τους απομνημονεύει. Οι κωδικοί ασφαλείας συνιστάται να είναι μήκους τουλάχιστον οκτώ (8) χαρακτήρων και να περιλαμβάνουν αλφαριθμητικά (αριθμούς, πεζά και κεφαλαία γράμματα) και σημεία στίξης.
7. Ο Προϊστάμενος της Υπηρεσίας να ενημερώνει άμεσα και εγγράφως τη Δ.Δ.Η.Δ. σχετικά με την αποχώρηση/μετάθεση υπαλλήλου από την Υπηρεσία, έτσι ώστε να γίνεται αφαίρεση των δικαιωμάτων πρόσβασης του υπαλλήλου στις εφαρμογές και τα υπηρεσιακά αρχεία.
8. Να κλειδώνει με μυστικό προσωπικό κωδικό την επιφάνεια εργασίας του Η/Υ του όταν απουσιάζει από το γραφείο του.
9. Κάθε χρήστης κατά τη διάρκεια του ωραρίου εργασίας, θα πρέπει να αποσυνδέεται στο προσωπικό του υπολογιστικό σύστημα (είτε με τη χρήση της λειτουργίας «εξόδου», ή μέσω απενεργοποίησης οθόνης, log out κ.τ.λ.), ανάλογα τα χρονικά διαστήματα απουσίας από τη θέση εργασίας του (αξιοποίηση του "time-outsession").
10. Εφόσον περιέλθει στην κατοχή του Π.Σ&Π.Τ που περιέχει ανοικτά αρχεία τρίτου προσώπου (λ.χ. χρήση Η/Υ υπαλλήλου που συνταξιοδοτήθηκε με όλα τα προσωπικά και υπηρεσιακά περιεχόμενα) οφείλει να ενημερώσει αρμοδίως για το γεγονός τη Δ.Δ.Η.Δ.

Ε. ΔΙΑΧΕΙΡΙΣΗ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

1. Τα υπηρεσιακά ψηφιακά αρχεία πρέπει να αποθηκεύονται στους αφιερωμένους για το σκοπό αυτό εξυπηρετητές και όχι στους προσωπικούς Η/Υ, καθώς στην πρώτη περίπτωση υπάρχει μέριμνα για τακτική λήψη αντιγράφων ασφαλείας. Αντίθετα, στη δεύτερη περίπτωση όπου ο χρήστης επιλέξει να αποθηκεύσει υπηρεσιακά ψηφιακά αρχεία στον προσωπικό του Η/Υ, οφείλει ο ίδιος να λαμβάνει μέριμνα για την ασφάλεια των ψηφιακών υπηρεσιακών φακέλων και εγγράφων του. Μάλιστα, στην περίπτωση αυτή ο υπάλληλος αποτελεί αυτοτελώς Υπεύθυνο Επεξεργασίας των δεδομένων που επεξεργάζεται και έχει όλες τις υποχρεώσεις που προβλέπονται από το κανονιστικό πλαίσιο για την προστασία των δεδομένων, συμπεριλαμβανομένης της λήψης μέτρων για την προστασία τους και της τήρησης των θεμελιωδών αρχών για την προστασία των προσωπικών δεδομένων.
2. Να λαμβάνει μέριμνα για την προστασία των αρχείων από μόλυνση από ιούς γνωρίζοντας ότι σε περίπτωση μόλυνσης υπάρχει κίνδυνος μη αναστρέψιμης απώλειας υπηρεσιακών αρχείων.
3. Να συνδέεται με τους κοινόχρηστους φακέλους της Υπηρεσίας στους οποίους έχει πρόσβαση μετά από άδεια της Υπηρεσίας, γνωρίζοντας ότι η όποια ενέργεια (π.χ. διαγραφή αρχείου) επηρεάζει τη λειτουργία όλων των υπαλλήλων που έχουν κοινή πρόσβαση στον κοινόχρηστο φάκελο.

4. Κατά την αντικατάσταση ή παράδοση Η/Υ από μία Υπηρεσία σε άλλη, απαιτείται η φύλαξη όλων των χρήσιμων υπηρεσιακών δεδομένων από την παραδίδουσα Υπηρεσία και, εν συνεχεία, η διαγραφή όλων των δεδομένων από τον Η/Υ με ευθύνη της Δ.Δ.Η.Δ.
5. Με την αποχώρηση/μετάθεση μέλους του προσωπικού της Π.Δ.Ε. από την Υπηρεσία, το μέλος υποχρεούται να μη διαγράψει ή αλλοιώσει τα υπηρεσιακά αρχεία και ηλεκτρονικά μηνύματα που είχε λάβει ή αποστείλει υπό την υπηρεσιακή του ιδιότητα ή είχε ο ίδιος δημιουργήσει κατά την εργασία του. Τα ψηφιακά αυτά στοιχεία πρέπει να είναι διαθέσιμα στον άμεσο Προϊστάμενό του.

Με την ανάγνωση της παρούσας Πολιτικής, οι υπόχρεοι αναγνωρίζουν οίκοθεν την προσωπική ευθύνη από ενδεχόμενη παραβίαση της ορθολογικής χρήσης των Πληροφοριακών Συστημάτων και Πληροφορικής Τεχνολογίας (Π.Σ.&Π.Τ.) της Π.Δ.Ε., παραβίαση η οποία μπορεί να διαπιστωθεί από την παρακολούθηση των ψηφιακών ιχνών κακής χρήσης και αθέτησης των όρων και προϋποθέσεων λειτουργίας τους. Επίσης, θεωρείται ότι έχουν λάβει γνώση των επιπτώσεων που συνεπάγεται οποιαδήποτε προσβολή των Π.Σ&Π.Τ. καθώς και του συνακόλουθου κόστους αποκατάστασης των υπεισερχομένων βλαβών/φθορών και της λειτουργικότητας, καθώς η παραμικρή δυσλειτουργία, διακοπή ή παράνομη διείσδυση στα συστήματα αυτά μεταφράζεται σε: α) κόστος οικονομικών απαιτήσεων αποκατάστασης, και β) αδυναμία αποδοτικής λειτουργίας του Φορέα.

Περαιτέρω, βάσει της παρούσας Πολιτικής, θεωρείται αποδεκτό για τους υπόχρεους, ότι εκτός από τις παραπάνω επιπτώσεις αποκατάστασης και επίλυσης των προβλημάτων ασφαλείας των πληροφοριακών συστημάτων της Π.Δ.Ε. προκύπτουν και νομικές ευθύνες από την αθέτηση περιφρούρησης και ορθής χρήσης του υπηρεσιακού εξοπλισμού και των υπηρεσιακών αρχείων που περιέχουν ευαίσθητα δεδομένα, ή επιτελούν ευαίσθητες και σημαντικές λειτουργίες. Οι ευθύνες αυτές, εμπίπτουν ευθέως στις διατάξεις τόσο του ποινικού όσο και του ισχύοντος πειθαρχικού δικαίου που αναφέρονται στο προοίμιο της παρούσας.

Οι Προϊστάμενοι των Υπηρεσιών μπορούν να διατυπώνουν προφορικά ή και γραπτά ενδεχόμενα ερωτήματα ερμηνείας και επεξηγήσεων επί της πολιτικής ασφαλείας των Π.Δ.&Π.Τ. προς τη Δ.Δ&Η.Δ. Μπορούν, επίσης, να ενημερωθούν περαιτέρω διαδικτυακά στον ιστότοπο του Υπουργείου Ψηφιακής Διακυβέρνησης https://mindigital.gr/kyvernoasfaleia [2].

Τέλος, μπορούν να επικοινωνήσουν με τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ – DPO) που έχει διορίσει η Π.Δ.Ε. στο emaildpo@pde.gov.grή στο τηλέφωνο 210-6819236.

[2]Σχετικό υλικό για τα μέτρα προστασίας πληροφοριακών συστημάτων από ηλεκτρονικές επιθέσεις στην Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025 https://tinyurl.com/fz68s4ne