ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΜΕΤΑΝΑΣΤΕΥΣΗΣ & ΑΣΥΛΟΥ
ΥΠΗΡΕΣΙΑΚΗ ΓΡΑΜΜΑΤΕΙΑ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΘΕΜΑ: «Εγκύκλιος Πολιτικών Ασφαλείας του Υπουργείου Μετανάστευσης και Ασύλου»

ΣΧΕΤ. :

α) π.δ. 106/2020 (Α' 255) «Οργανισμός του Υπουργείου Μετανάστευσης και Ασύλου, όπως αυτό τροποποιήθηκε και ισχύει με το π.δ. 77/2022 (Α’ 212), το π.δ. 20/2023(Α’ 43) και το π.δ. 77/2023 (Α’ 130).

β) Ν. 4577/2018 (Α΄ 199) «Ενσωμάτωση Οδηγίας 2016/1148/ΕΕ σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις - γνωστή ως Οδηγία NIS»

γ) Ν. 4624/2019 (Α΄ 137) «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις»,

δ) Διατάξεις:

α. του ν. 2690/1999 «Κώδικας Διοικητικής και Διαδικασίας» (Α’ 45), όπως ισχύει,

β. των άρθρων 25 και 84 του ν. 3528/2007 «Κύρωση του Κώδικα κατάστασης Δημόσιων Πολιτικών Υπαλλήλων και Υπαλλήλων ΝΠΔΔ» (Α’ 26), όπως ισχύουν,

γ. των άρθρων 2 έως 6 του ν. 3861/2010 «Ενίσχυση της διαφάνειας με την υποχρεωτική ανάρτηση νόμων και πράξεων των κυβερνητικών, διοικητικών και αυτοδιοικητικών οργάνων στο διαδίκτυο «Πρόγραμμα Διαύγεια» και άλλες διατάξεις» (Α’ 112), όπως ισχύει,

δ. του ν. 3979/2011 «Για την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις» (Α’ 138), όπως ισχύει και ειδικότερα την παράγραφο 10 του άρθρου 12,

στ. του ν. 4727/2020 Ψηφιακή Διακυβέρνηση(Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας(ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ)2019/1024) Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ)201/1972 και άλλες διατάξεις, όπως τροποποιήθηκε και ισχύει,

ζ. του Κανονισμού Επικοινωνίας Δημοσίων Υπηρεσιών (Υπουργείο Εσωτερικών Δημόσιας Διοίκησης και Αποκέντρωσης, Γενική Γραμματεία Δημόσιας Διοίκησης, Ιανουάριος 2003) και τον Κανονισμό Επικοινωνίας Υπηρεσιών (Κεντρική Ένωση Δήμων και Κοινοτήτων Ελλάδος, Οκτώβριος 2007).

Γνωρίζεται ότι, σύμφωνα με το άρθρο 17 του (α) σχετικού, η Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών, είναι μεταξύ άλλων αρμόδια για τον σχεδιασμό και την εφαρμογή α) πολιτικών ασφάλειας του ενδοδικτύου και των πληροφοριακών δεδομένων και β) των διαδικασιών εναρμόνισης των πληροφοριακών συστημάτων του Υπουργείου με εθνικά και διεθνή πρότυπα ασφάλειας, καθόσον είναι η καθ' ύλην αρμόδια Υπηρεσία για την διαδικασία της επεξεργασίας των δεδομένων.

Με τις πολιτικές ασφαλείας καθορίζεται ένα ελάχιστο βασικό επίπεδο ασφαλείας των πληροφοριακών συστημάτων και των πληροφοριακών δεδομένων όχι μόνο σε ότι αφορά την κεντρική υποδομή του Φορέα αλλά περιλαμβάνει και τα συστήματα – υποδομή που χρησιμοποιούνται από τους χρήστες ήτοι τα στελέχη του κατά την ενάσκηση των καθημερινών καθηκόντων τους, με απώτερο τελικό σκοπό την εξασφάλιση της προστασίας από κάθε είδους απειλή, τυχαία ή σκόπιμη.

Οι προαναφερόμενες Πολιτικές Ασφαλείας κατόπιν ολοκλήρωσης της ανάπτυξης και επεξεργασίας τους από την ορισθείσα Ομάδα Εργασίας μετά την υποβολή της στην αρμόδια - επισπεύδουσα Υπηρεσία, επισυνάπτονται στο παρόν στην τελική της μορφή. Το πεδίο εφαρμογής της εν λόγω εγκυκλίου αφορά στην ενημέρωση του συνόλου των στελεχών και Υπηρεσιών του Φορέα καθώς και των συνεργαζόμενων με το Φορέα, φυσικών και νομικών προσώπων.

Κατόπιν των προαναφερόμενων, με ευθύνη και με την επίδειξη της δέουσας υπευθυνότητας, επιμέλειας και συνέπειας των κ.κ. Διευθυντών ή Προϊσταμένων των Οργανικών Μονάδων του Υπουργείου, παρακαλούνται για την ενυπόγραφη ενημέρωση όλου του προσωπικού, σύμφωνα με το έντυπο στο Παράρτημα VI, το οποίο θα φυλάσσεται στα αρχεία των Οργανικών τους μονάδων με σκοπό την τήρηση των μέτρων ασφαλείας Πληροφοριακών Συστημάτων όπως αυτά περιγράφονται.

Ο Προϊστάμενος της Γενικής Διεύθυνσης Πληροφορικής & Επικοινωνιών

Δρ. Αναστάσιος Σαλής

Η Υπηρεσιακή Γραμματέας

Ουρανία Σταυροπούλου

Ο Υπουργός

Δημήτρης Καιρίδης

Επισυνάπτεται: Οι Πολιτικές Ασφαλείας του ΥΜΑ

ΠΙΝΑΚΑΣ ΔΙΑΝΟΜΗΣ :

Ι. ΑΠΟΔΕΚΤΕΣ ΓΙΑ ΕΝΕΡΓΕΙΑ :

Όλες οι Υπηρεσίες του Υπουργείου.

ΙΙ. ΕΣΩΤΕΡΙΚΗ ΔΙΑΝΟΜΗ :

Γραφεία Πολιτικής Ηγεσίας

Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών

ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

ΥΜΑ

Περιεχόμενα

ΑΚΡΩΝΥΜΙΑ

Υπουργείο Μετανάστευσης και Ασύλου	Υ.Μ.Α.
Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών του Υπουργείου Μετανάστευσης και Ασύλου	Γ.Δ. Πληροφορικής και Επικοινωνιών Υ.Μ.Α.
Γενικός Κανονισμός Προστασίας Δεδομένων	Γ.Κ.Π.Δ.- GDPR
Πληροφοριακά Συστήματα	Π.Σ.
Εθνικός Κανονισμός Ασφαλείας	Ε.Κ.Α.
Υπεύθυνος Επεξεργασίας	Υ.Ε.
Υπεύθυνος Προστασίας Δεδομένων	DPO
Εκτελών της Επεξεργασίας	Ε.Ε.
Αρχή Επιχειρησιακής Λειτουργίας	Α.Ε.Λ.
Υπεύθυνος Ασφάλειας Συστημάτων	Υ.Α.Σ.
Υπεύθυνος Ασφάλειας Δικτύου	Υ.Α.Δ.
Υπεύθυνος Ασφάλειας Τοποθεσίας	Υ.Α.Τ.
Κλειστό Κύκλωμα Παρακολούθησης	CCTV
Σύστημα Ηλεκτρονικής Διακίνησης Εγγράφων	ΙΡΙΔΑ
Εφαρμογή Χαρτογράφησης Αλλοδαπών	ΑΛΚΥΟΝΗ
Ελληνική Αστυνομία	ΕΛ.ΑΣ.
Δίκτυο Ελληνικής Αστυνομίας	POL

1. Εισαγωγή – Στοχοθεσία Πολιτικής Ασφαλείας

Η Πολιτική Ασφάλειας της Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών του Υπουργείου Μετανάστευσης και Ασύλου (Υ.Μ.Α.) περιγράφει και επικυρώνει το σύνολο των κανόνων ασφαλείας και τις αντίστοιχες διαδικασίες, η εφαρμογή των οποίων στοχεύει στην προστασία των Διαδικτυακών Υποδομών, των Πληροφοριακών Συστημάτων και των Δεδομένων που διαχειρίζεται το Υ.Μ.Α. Ταυτόχρονα, ο φορέας δεσμεύεται μέσω της Πολιτικής Ασφαλείας για τις υποχρεώσεις του βάσει του ρυθμιστικού συστήματος και του κανονιστικού πλαισίου που επιτάσσει ο νέος Ευρωπαϊκός Κανονισμός Προστασίας Δεδομένων και διατηρεί ένα ισχυρό και δομημένο πρόγραμμα συμμόρφωσης και παρακολούθησης των υπηρεσιακών του διαδικασιών που εμπεριέχουν επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Προτεραιότητα του Υ.Μ.Α είναι η προστασία όλων των επιχειρησιακών δεδομένων και ιδιαίτερα των προσωπικών ή των ευαίσθητων προσωπικών δεδομένων από εκούσια ή ακούσια κλοπή, καταστροφή ή χρήση κατά παράβαση των Νόμων και των Κανονιστικών Διατάξεων.

Ως εκ τούτου, η εμπιστευτικότητα, η ακεραιότητα και η υψηλή διαθεσιμότητα των πληροφοριών έχει ως σκοπό την ασφάλεια και την προστασία των δεδομένων του Υ.Μ.Α, καθώς και τον περιορισμό των κινδύνων που απειλούν τα δεδομένα του.

Η συγκεκριμένη Πολιτική Ασφαλείας περιλαμβάνει τις θεμελιώδεις αρχές που πρέπει να ισχύουν για την ασφάλεια των πληροφοριών, των Πληροφοριακών Συστημάτων, του δικτυακού εξοπλισμού, της κτιριακής υποδομής, των συστημάτων παρακολούθησης (CCTV), της φύλαξης εξοπλισμού και των χώρων εργασίας. Η τήρηση των οριζόμενων αρχών είναι απαραίτητη για την αποτελεσματική διαχείριση του υφιστάμενου υπηρεσιακού πληροφοριακού υλικού για την επαρκή προστασία του οργανισμού από κακόβουλη δραστηριότητα είτε εκ των έσω, είτε από τρίτους είτε από φυσικές καταστροφές.

Η Πολιτική Ασφάλειας διαμορφώθηκε σύμφωνα με τις βέλτιστες πρακτικές και τα διεθνή πρότυπα (COBIT, ISO/IEC 17799, ISO 27001/27002, NIST) και παραμένει άρρηκτα συνδεδεμένη με τη φύση των δραστηριοτήτων του Υ.Μ.Α, τις κατευθυντήριες γραμμές της Διοίκησης και το επιχειρησιακό περιβάλλον. Ως προς τη διάρθρωση της δομής της ακολουθεί ένα ενιαίο μοντέλο περιγραφής των κανόνων ασφαλείας και των διαδικασιών και όπου κρίνεται απαραίτητη η εξειδίκευση αυτών, για συγκεκριμένα υποσυστήματα επεξεργασίας δεδομένων, εμπλουτίζεται με αντίστοιχα παραρτήματα. Βασικά σημεία για τη βέλτιστη κατανόηση και αξιοποίηση της Πολιτικής Ασφάλειας αποτελούν οι εξής διαπιστώσεις:

- Η Πολιτική Ασφάλειας αποτελεί για τα στελέχη και τους εργαζόμενους του Υ.Μ.Α βασικό μέσο διαμόρφωσης κουλτούρας συμμόρφωσης με τους κανόνες ασφαλείας. Επιπλέον, διατίθεται ως υπηρεσιακό έγγραφο και όλα τα εμπλεκόμενα μέλη που έχουν ενεργό ρόλο στη λειτουργία των πληροφοριακών υποδομών, ως χρήστες, ως διαχειριστές ή ως διοικητικά στελέχη, λαμβάνουν επαρκή γνώση αυτής.
- Η Πολιτική Ασφάλειας δεν είναι στατική, εξελίσσεται και επικαιροποιείται συνεχώς προκειμένου να καλύπτει το σύνολο των αναγκών που προκύπτουν. Βασίζεται στην ανάλυση των αποκλίσεων του Γενικού Κανονισμού για την Προστασία Δεδομένων

(Γ.Κ.Π.Δ.-GDPR), καθώς και στις βασικές κατευθυντήριες γραμμές, στις βέλτιστες πρακτικές, στα διεθνή πρότυπα και στους εθνικούς κανόνες ασφαλείας.

- Η Πολιτική Ασφάλειας είναι ευέλικτη και δυναμική. Το ακριβές πεδίο εφαρμογής, το ύφος και το περιεχόμενο της Πολιτικής αυτής ορίζεται, βάσει των εκάστοτε προτεραιοτήτων του Υπουργείου, οι οποίες αναδιαμορφώνονται βάσει των υπηρεσιακών εξελίξεων.

1.1 Εφαρμογή και Επικαιροποίηση Πολιτικής Ασφαλείας

Χαρακτηριστικά Πολιτικής Ασφαλείας			
Όνομα Πολιτικής	Πολιτική Ασφάλειας Γ.Δ. Πληροφορικής και Επικοινωνιών Υπουργείου Μετανάστευσης και Ασύλου	**Δημιουργία**	19/04/2024
Είδος Πολιτικής	Γενική Πολιτική Ασφάλειας	**Κοινό**	Δημόσιο
Οργανισμός	Υπουργείο Μετανάστευσης και Ασύλου	**Έκδοση**	1.0

Η Πολιτική Ασφάλειας τίθεται σε εφαρμογή και ελέγχεται ως προς την εφαρμογή της από τη Διοίκηση του Υ.Μ.Α. και το Τμήμα Ασφάλειας Πληροφοριών, Συστημάτων και Εφαρμογών του Υ.Μ.Α. Κάθε εργαζόμενος ο οποίος παραβιάζει την παρούσα, δύναται να υποστεί κυρώσεις εξ αυτού του λόγου. Σε περίπτωση που διαπιστωθούν έκνομες δραστηριότητες με απώτερο σκοπό την εκμετάλλευση των περιουσιακών στοιχείων του Υ.Μ.Α., εκκινείται διαδικασία από τις αρμόδιες πειθαρχικές αρχές. Ειδικότερα, η ειδική έννομη σχέση η οποία συνδέει τον υπάλληλο με το Κράτος, σχετίζεται με την ορθή εκτέλεση των καθηκόντων του και τυχόν πειθαρχική ευθύνη ρυθμίζεται από τις διατάξεις του πειθαρχικού δικαίου, το οποίο αποτελεί κομμάτι του Υπαλληλικού Κώδικα. Στο αρ. 109 του Ν. 3528/2007, όπως αυτό ισχύει μετά την αντικατάστασή του από τους Ν. 4057/2012 και 4325/2015, προβλέπονται, κατά τρόπο περιοριστικό, οι πειθαρχικές ποινές. Πειθαρχικά παραπτώματα όπως για παράδειγμα, η παραβίαση της υποχρέωσης εχεμύθειας (άρθρο 26 Υ.Κ.) και η χρησιμοποίηση της δημοσιοϋπαλληλικής ιδιότητας ή πληροφοριών που κατέχει ο υπάλληλος λόγω της υπηρεσίας ή της θέσης του προς εξυπηρέτηση ιδιωτικών συμφερόντων του ίδιου ή τρίτων, επισύρουν πειθαρχικές ποινές ή κυρώσεις.

Ο παρακάτω πίνακας συμπληρώνεται κάθε φορά που προκύπτει αλλαγή ή ενόψει της προγραμματισμένης επικαιροποίησης αυτής. Αρμόδιο τμήμα για την εκτέλεση της προαναφερθείσας διαδικασίας είναι το Τμήμα Ασφάλειας Πληροφοριών, Συστημάτων και Εφαρμογών.

Ιστορικό εκδόσεων		
Υπεύθυνος	**Ημερομηνία**	**Περιγραφή**
Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών	19/04/2023	1η έκδοση

1.2 Στόχος

Βασικός στόχος της παρούσας πολιτικής είναι να διαμορφώσει ένα ενιαίο πλαίσιο Ασφάλειας για τα Πληροφοριακά Συστήματα και Δεδομένα (Προσωπικά & Υπηρεσιακά) του Υ.Μ.Α. Το ενιαίο πλαίσιο Ασφαλείας περιλαμβάνει, πέρα από τα υπάρχοντα τεχνολογικά εργαλεία, μεθόδους, κανόνες αλλά και μηχανισμούς επιβολής της εν λόγω Πολιτικής.
Επιπλέον στόχοι της παρούσας πολιτικής είναι:

- Η συμμόρφωση με το νομοθετικό και κανονιστικό πλαίσιο που αφορά την προστασία προσωπικών δεδομένων, όπως επιτάσσει ο Γενικός Κανονισμός για την Προστασία Δεδομένων (Γ.Κ.Π.Δ.-GDPR)
- Η διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας πληροφοριών και επικοινωνιών
- Η προστασία των λειτουργικών πόρων που απαιτεί η λειτουργία των Πληροφοριακών Συστημάτων (Π.Σ.)
- Η αποτροπή μη εξουσιοδοτημένης φυσικής πρόσβασης, υλικών ζημιών και κακόβουλων ενεργειών πάσης φύσεως στις εγκαταστάσεις
- Ο καθορισμός της διαβαθμισμένης πρόσβασης όλων των εμπλεκόμενων προσώπων του Υπουργείου στους πληροφοριακούς πόρους
- Ο καθορισμός κανόνων για τη σύνδεση με το δίκτυο του Υπουργείου από οποιονδήποτε υπηρεσιακό υπολογιστή (ή κινητά τηλέφωνα, tablet, φορητούς υπολογιστές)
- Η ενημέρωση και η δέσμευση του προσωπικού του Υπουργείου, στους οποίους έχουν χορηγηθεί συσκευές και εξοπλισμός για την εκτέλεση των υπηρεσιακών εργασιών τους
- Η ενημέρωση και η δέσμευση των εργαζομένων, στους οποίους έχουν χορηγηθεί υπηρεσιακοί λογαριασμοί mail για την τήρηση των κανόνων πρόσβασης τόσο στο διαδίκτυο όσο και εντός υπηρεσιακού δικτύου
- Η αποτύπωση των απαιτούμενων μέτρων ασφάλειας που διαθέτει το Υπουργείο για την προστασία των δικτυακών επικοινωνιών από ακούσιες ή εκούσιες εξωτερικές απειλές
- Ο καθορισμός των κανόνων και διαδικασιών ώστε να εξασφαλιστεί ότι τα αντίγραφα ασφάλειας λαμβάνονται και τηρούνται σύννομα και με ασφάλεια
- Η θέσπιση κατάλληλων διαδικασιών, ελέγχων και μέτρων αλλά και η έγκαιρη γνωστοποίησή τους σε όλους τους εργαζομένους και η ορθή εφαρμογή τους από αυτούς
- Η θέσπιση ενός πλάνου αντιμετώπισης περιστατικών παραβίασης
- Ο καθορισμός των διαδικασιών και μεθόδων κρυπτογράφησης
- Ο καθορισμός απαιτήσεων σχετικά με τους κωδικούς πρόσβασης

1.3 Πεδίο εφαρμογής - αποδέκτες

Η παρούσα Πολιτική έχει εφαρμογή σε όλα τα Πληροφοριακά Συστήματα (Π.Σ.) και εφαρμογές του Υ.Μ.Α., όπως αυτά αποτυπώνονται παρακάτω:

- Ενιαίο Πληροφοριακό Σύστημα Υποδοχής και Ασύλου (Αλκυόνη ΙΙ)
- ΟΠΣ «Νόμιμη Μετανάστευση»
- Σύστημα Ηλεκτρονικής Διακίνησης Εγγράφων – ΙΡΙΔΑ
- Εφαρμογές Office 365
- Εφαρμογές που έχουν αναπτυχθεί εντός του Οργανισμού (In-house) όπως το Σύστημα Υποστήριξης Υπηρεσιών Πληροφορικής – ΑΤΛΑΣ και η Εφαρμογή Επιτροπείας.
- Λοιπά λειτουργικά συστήματα και εφαρμογές

Τα αυτόνομα ολοκληρωμένα Π.Σ. λειτουργούν βάσει εξειδικευμένων Σχεδίων Ασφάλειας, με την προϋπόθεση ότι αυτά συμμορφώνονται με τις βασικές αρχές του Ε.Κ.Α. Όλο το προσωπικό του Υ.Μ.Α με οποιαδήποτε σχέση εργασίας αλλά και οι χρήστες άλλων Φορέων-Οργανισμών (εφόσον κάνουν χρήση των συστημάτων-δεδομένων του Υ.Μ.Α., είτε απευθείας ή μέσω άλλων συστημάτων) υποχρεούνται να συμμορφώνονται ως προς τις απαιτήσεις της παρούσας Πολιτικής και να συμβάλλουν στην ενίσχυση των πρακτικών ασφαλείας, συνειδητοποιώντας τις υποχρεώσεις που έχουν στο πλαίσιο της ισχύουσας νομοθεσίας για την προστασία προσωπικών δεδομένων και την ασφάλεια των Π.Σ. Ταυτόχρονα, οι εργαζόμενοι, οι εξωτερικοί συνεργάτες, οι επισκέπτες και άλλα ενδιαφερόμενα μέλη συμπεριλαμβάνονται τόσο στο πεδίο εφαρμογής όσο και στο σύνολο των αποδεκτών της εν λόγω Γενικής Πολιτικής Ασφαλείας.

1.4 Ρόλοι και αρμοδιότητες

Στο συγκεκριμένο εδάφιο καθορίζεται το οργανωτικό πλαίσιο ασφαλείας δηλαδή οι βασικοί και επικουρικοί ρόλοι που σχετίζονται με την ασφάλεια των Π.Σ., των Διαδικτυακών Υποδομών και πληροφοριών του Υ.Μ.Α. και ταυτόχρονα περιγράφονται οι αντίστοιχες αρμοδιότητες και τα καθήκοντα αυτών, σύμφωνα με το επίσημο οργανόγραμμα του Οργανισμού (Προεδρικό Διάταγμα υπ' αριθμ. 106 όπως αυτό τροποποιήθηκε και ισχύει με τα π.δ. 77/2022 (Α' 212), π.δ. 20/2023(Α' 43 και π.δ. 77/2023 (Α' 130)) και τον Ε.Κ.Α.

Ρόλος	Περιγραφή	Πρόσωπο/Τμήμα
Υπεύθυνος Επεξεργασίας	Ο Υπεύθυνος Επεξεργασίας ως κάτοχος των δεδομένων του οργανισμού ορίζει τους σκοπούς και τους τρόπους επεξεργασίας τους και καθορίζει τις επιχειρησιακές στρατηγικές διαχείρισης αυτών από τα αντίστοιχα Π.Σ..	Υ.Μ.Α.
Υπεύθυνος Προστασίας Δεδομένων	Ο Υπεύθυνος Προστασίας Δεδομένων ορίζεται από τη Διοίκηση του Οργανισμού και αναλαμβάνει την παροχή συμβουλευτικών υπηρεσιών σε ζητήματα που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα. Βασικός του ρόλος είναι να διευκολύνει τη συμμόρφωση του υπευθύνου	Εξωτερικός συνεργάτης. «ΕΥΡΩΑΞΟΝΕΣ ΚΑΙΝΟΤΟΜΕΣ ΤΕΧΝΟΛΟΓΙΚΕΣ & ΣΥΜΒΟΥΛΕΥΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ Α.Ε.

	επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του Γενικού Κανονισμού Προσωπικών Δεδομένων και μεσολαβεί μεταξύ των διαφόρων εμπλεκομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων).	
Εκτελών της Επεξεργασίας	Ο Εκτελών της Επεξεργασίας είναι το φυσικό ή νομικό πρόσωπο, ή δημόσια αρχή, ή υπηρεσία, ή άλλος φορέας που του έχει ανατεθεί από τον Υπεύθυνο της Επεξεργασίας η επεξεργασία των δεδομένων. Σημειώνεται πως με απόφαση του Υπεύθυνου Επεξεργασίας δύναται να υπάρχουν παραπάνω του ενός εκτελούντες της επεξεργασίας, ενώ προβλέπεται και το ενδεχόμενο ο Υπεύθυνος Επεξεργασίας να λειτουργεί άλλοτε ως ο υπεύθυνος και άλλοτε ως ο εκτελών της επεξεργασίας (άρθρο 4 περ. 7, άρθρο 4 περ. 8 του Γ.Κ.Π.Δ.- GDPR) .	Εταιρείες - Ανάδοχοι
Επόπτης Ασφάλειας Πληροφοριακών Συστημάτων και Δικτύου	Ο Επόπτης Ασφάλειας Πληροφοριακών Συστημάτων και Δικτύου αναλαμβάνει και συνδιαμορφώνει με την Α.Ε.Λ. τις γενικές κατευθύνσεις για την ασφάλεια των Π.Σ. και των Δικτυακών Υποδομών του Οργανισμού και υποστηρίζει τον έλεγχο εφαρμογής και τήρησης αυτών. Στο πλαίσιο αυτό ορίζεται ως συντονιστής όλων των υπευθύνων.	Τμήμα Ασφάλειας Πληροφοριών, Συστημάτων και Εφαρμογών.
Αρχή Επιχειρησιακής Λειτουργίας	Η Αρχή Επιχειρησιακής Λειτουργίας/ Α.Ε.Λ. όλων των Π.Σ. του Οργανισμού συστήνεται από προϊσταμένους των Οργανικών Μονάδων της Γ.Δ. Πληροφορικής και Επικοινωνιών και έχει ως κύριο έργο τη διαμόρφωση και τον έλεγχο όλων των διαδικασιών που άπτονται στους τομείς της σχεδίασης, ανάπτυξης, διασύνδεσης και ασφάλειας των Π.Σ. και των Δικτυακών Υποδομών του Οργανισμού.	Προϊστάμενος της Γ.Δ. Πληροφορικής και Επικοινωνιών καθώς και οι Προϊστάμενοι όλων των Διευθύνσεων και Τμημάτων της Γ.Δ. Πληροφορικής και Επικοινωνιών.
Υπεύθυνος Ασφάλειας Συστημάτων	Ο Υπεύθυνος Ασφάλειας Συστημάτων είναι αρμόδιος για τον έλεγχο τήρησης της Πολιτικής Ασφαλείας και υπεύθυνος για θέματα προστασίας των προσωπικών δεδομένων, όσον αφορά στις αρχές της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας αυτών.	Προϊστάμενος Τμήματος Λογισμικού και Επιχειρησιακών Εφαρμογών. Ελλείψει Προϊσταμένου Τμήματος Λογισμικού και Επιχειρησιακών Εφαρμογών ως Υ.Α.Σ.

		ορίζεται ο Προϊστάμενος της Διεύθυνσης Εφαρμογών Πληροφορικής και Επικοινωνιών.
Υπεύθυνος Ασφάλειας Δικτύου	Ο Υπεύθυνος Ασφάλειας Δικτύου είναι αρμόδιος για την εφαρμογή των αρχών και προτύπων ασφαλείας των Υποδομών, των δικτυακών και υπολογιστικών πόρων από εσωτερικές, εξωτερικές απειλές και κινδύνους, σε συνεργασία με το Τμήμα Ασφάλειας Πληροφοριών, Συστημάτων και Εφαρμογών και την Α.Ε.Λ.	Προϊστάμενος Τμήματος Διαχείρισης Υποδομών. Ελλείψει Προϊσταμένου Τμήματος Διαχείρισης Υποδομών ως Υ.Α.Δ. ορίζεται ο Προϊστάμενος της Διεύθυνσης Υποδομών Πληροφορικής και Επικοινωνιών (επιτελικός ρόλος).
Υπεύθυνος Ασφάλειας Τοποθεσίας	Ο Υπεύθυνος Ασφάλειας Τοποθεσίας είναι αρμόδιος για την τήρηση των κανόνων ασφαλείας όσον αφορά τις φυσικές εγκαταστάσεις των Π.Σ. και των Δικτυακών Υποδομών του Οργανισμού σε συνεργασία με την Α.Ε.Λ., τους Υ.Α.Δ., Υ.Α.Σ. και το Τμήμα Ασφάλειας Πληροφοριών, Συστημάτων και Εφαρμογών.	Προϊστάμενος Τμήματος Διαχείρισης Υποδομών.
Ομάδα Αντιμετώπισης Περιστατικών Παραβίασης	Η Ομάδα Αντιμετώπισης Περιστατικών Παραβίασης σε συνεργασία με τις αρμόδιες Αρχές, είναι υπεύθυνη για τη διερεύνηση, την αξιολόγηση και την επίλυση των περιστατικών παραβίασης ασφαλείας. Βασική αρχή λειτουργίας της Ομάδας αυτής είναι η καταγραφή, η ανάλυση, η αξιολόγηση των διαδικασιών και λειτουργιών, η πληροφόρηση και η ενημέρωση των μελών, ο σχεδιασμός και η βελτίωση με βάση την εμπειρία που αποκτάται σε ό,τι αφορά τη διαχείριση περιστατικών ασφαλείας.	Στελέχη από το δυναμικό της Γ.Δ. Πληροφορικής και Επικοινωνιών σε συνεργασία με τις αρμόδιες Αρχές: Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΕΛ.ΑΣ.), Εθνικό CERT - ΕΥΠ, ΑΠΔΠΧ, κ.λπ.

Σχετικά με το Τμήμα Ασφάλειας Πληροφοριών, Συστημάτων και Δικτύου, που αποτελεί και τον επόπτη και τον συντονιστή όλων των ζητημάτων που αφορούν την ψηφιακή ασφάλεια επιφορτίζεται με τις παρακάτω αρμοδιότητες:

- Την παρακολούθηση και τη διαρκή ενημέρωση της εξέλιξης των τεχνολογιών σε θέματα ασφάλειας των συστημάτων πληροφορικής και επικοινωνιών
- Την εκπόνηση μελετών και τη διατύπωση προτάσεων για τη διαμόρφωση της πολιτικής και του σχεδίου ασφάλειας που εφαρμόζεται από το Υ.Μ.Α.
- Τον σχεδιασμό και την εφαρμογή πολιτικών ασφάλειας του δικτύου και των πληροφοριακών δεδομένων, ιδίως από καταστροφή, απώλειες, μη εξουσιοδοτημένη πρόσβαση και χρήση, αλλοίωση περιεχομένου, κακόβουλο λογισμικό, καθώς και τον σχεδιασμό και την εφαρμογή πολιτικών προστασίας προσωπικών δεδομένων και όλων των λοιπών δεδομένων που τηρούνται σε ψηφιακή μορφή στις υπηρεσίες του Υ.Μ.Α. από μη εξουσιοδοτημένη πρόσβαση και χρήση
- Την παρακολούθηση της εφαρμογής του σχεδίου ασφάλειας και την αξιολόγηση της αποτελεσματικότητάς του
- Τον σχεδιασμό και την εφαρμογή διαδικασιών εναρμόνισης των πληροφοριακών συστημάτων του Υ.Μ.Α. με εθνικά και διεθνή πρότυπα ασφάλειας
- Την ταυτοποίηση και αυθεντικοποίηση των χρηστών των ηλεκτρονικών συστημάτων του Υ.Μ.Α., σύμφωνα με τις απαιτήσεις και τις εκάστοτε ισχύουσες γενικές τεχνικές προδιαγραφές, όπως ενδεικτικά αναφέρονται το «Πλαίσιο Ψηφιακής Αυθεντικοποίησης» και το «Πλαίσιο Διαλειτουργικότητας και Ηλεκτρονικών Συναλλαγών»
- Τη σύνταξη περιοδικών αναφορών και εκθέσεων ασφάλειας, καθώς και ετήσιας απολογιστικής έκθεσης σχετικά με την αποτελεσματικότητα του σχεδίου ασφάλειας
- Την επιμέλεια για την ορθή εφαρμογή της νομοθεσίας για την προστασία δεδομένων προσωπικού χαρακτήρα και γενικά των διαβαθμισμένων πληροφοριών
- Την κατάρτιση, εξειδίκευση και εποπτεία της εφαρμογής γενικών τεχνικών και λειτουργικών προτύπων διαλειτουργικότητας, ασφάλειας, προστασίας και ακεραιότητας δεδομένων των πληροφοριακών συστημάτων του Υ.Μ.Α.
- Την εισήγηση νομοθετικών ρυθμίσεων και διοικητικών μέτρων με σκοπό τη διασφάλιση της τήρησης των τεχνικών και λειτουργικών προδιαγραφών και προτύπων
- Τη συνεργασία με εθνικούς, ευρωπαϊκούς και διεθνείς οργανισμούς για την ασφάλεια δικτύων και πληροφοριών, την παρακολούθηση των σχετικών τεχνολογικών εξελίξεων, καθώς και την ενημέρωση του προσωπικού επί θεμάτων ασφαλείας
- Τη συνεργασία με τον Υπεύθυνο Προστασίας Δεδομένων (DPO)
- Τη δυνατότητα ορισμού ομάδας αποτελούμενης από στελέχη όλων των υπηρεσιών του Υ.Μ.Α., λαμβάνοντας υπόψη τις εξαιρέσεις που απορρέουν από την ερμηνεία του Γ.Κ.Π.Δ.(GDPR), ήτοι τους ρόλους του «Υπεύθυνου Επεξεργασίας», του «Εκτελούντος την επεξεργασία» ή την ανάθεση αυτού σε άλλο φορέα ή οργανισμό
- Τη συνεργασία με το Τμήμα Διοικητικής Μέριμνας και Προδιαγραφών της Διεύθυνσης Υποδομών Πληροφορικής και Επικοινωνιών σε όλα τα θέματα που απαιτείται, ώστε να εξασφαλίζεται η εφαρμογή των διεθνών καλών πρακτικών της κυβερνοασφάλειας.

2.Πολιτική Ασφάλειας Εγκαταστάσεων

2.1 Κύρια εγκατάσταση

Στο κτίριο Κεράνης υπάρχουν δύο είσοδοι, η κεντρική είσοδος από την οδό Θηβών και η είσοδος από το υπαίθριο πάρκινγκ επί της οδού Μάρκου Μπότσαρη. Και στις δύο εισόδους

βρίσκεται προσωπικό εταιρείας φύλαξης το οποίο είναι υπεύθυνο για την ταυτοποίηση των ατόμων.

Στον έκτο (6ο) όροφο του κτιρίου Κεράνης στεγάζεται η Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών. Η πρόσβαση πραγματοποιείται μέσω των δύο ανελκυστήρων που βρίσκονται στην αριστερή πλευρά της κεντρικής εισόδου. Η είσοδος στα γραφεία της Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών πραγματοποιείται μέσω κεντρικής πόρτας στην οποία η πρόσβαση είναι εφικτή μόνο με την **εισαγωγή της αντίστοιχης φυσικής ή ψηφιακής κάρτας,** την οποία κατέχουν μόνο εξουσιοδοτημένα άτομα. Σε λοιπές περιπτώσεις η πρόσβαση των ενδιαφερόμενων στα γραφεία της Γενικής Διεύθυνσης, γίνεται μέσω χρήσης εγκατεστημένου κουδουνιού και κάμερας, εφόσον τους χορηγηθεί η άδεια πρόσβασης. Το κέντρο δεδομένων (Computer Room) του Υ.Μ.Α. βρίσκεται και αυτό στον έκτο (6ο) όροφο σε ειδικά διαμορφωμένο χώρο που διαθέτει επιπλέον σύστημα πρόσβασης. Τέλος στον έκτο όροφο υπάρχει και δεύτερη πόρτα πρόσβασης, η οποία λειτουργεί μόνο ως έξοδος σε περιπτώσεις ανάγκης και δεν επιτρέπεται η είσοδος από αυτή.

2.2 Συστήματα ασφαλείας

Για την προστασία από περιβαλλοντικές απειλές (π.χ. φωτιά, πολύ υψηλές/χαμηλές θερμοκρασίες) χρησιμοποιούνται τα παρακάτω συστήματα:

- Συστήματα πυρανίχνευσης
- Κλιματισμός
- Πυροσβεστήρες ξηράς σκόνης

2.3.Κλειστό κύκλωμα παρακολούθησης (CCTV)

Στον έκτο (6ο) όροφο είναι τοποθετημένες εννέα (9) κάμερες με ζωντανή μετάδοση, εκ των οποίων στις επτά (7) έχει πρόσβαση η γραμματεία της Γενικής Διεύθυνσης Πληροφορικής, και στις υπολειπόμενες δύο (2) το κέντρο διαχείρισης συμβάντων. Επίσης, υπάρχει καταγραφικό στο οποία η πρόσβαση γίνεται μόνο από εξουσιοδοτημένα άτομα. Σε όλους τους χώρους της Γ.Δ. Πληροφορικής και Επικοινωνιών, έχουν τοποθετηθεί σημάνσεις ότι ο χώρος παρακολουθείται από κλειστό κύκλωμα παρακολούθησης (CCTV). Το rotation του καταγραφικού υλικού έχει οριστεί στις δεκαπέντε (15) ημέρες σύμφωνα με την κείμενη Νομοθεσία και δεν τηρείται επιπλέον backup. Επισημαίνεται δε ότι μετά την πάροδο των δεκαπέντε (15) ημερών, τα δεδομένα διαγράφονται αυτόματα. Σε περίπτωση που στο διάστημα αυτό διαπιστωθεί κάποιο περιστατικό, απομονώνεται τμήμα του βίντεο το οποίο τηρείται έως και έναν (1) επιπλέον μήνα, με σκοπό τη διερεύνηση του περιστατικού και την έναρξη νομικών διαδικασιών για την υπεράσπιση των εννόμων συμφερόντων του Υ.Μ.Α., ενώ σε περίπτωση που το περιστατικό αφορά τρίτον, το βίντεο τηρείται έως και τρεις (3) επιπλέον μήνες.

2.4 Κουζίνα

Λόγω της αυξημένης επικινδυνότητας του εν λόγω χώρου για την πρόκληση φυσικών καταστροφών στην υποδομή και το προσωπικό, ορίζεται η ακόλουθη Πολιτική:

Στον χώρο της κουζίνας εκτός από το σύστημα πυρανίχνευσης, υπάρχουν και πυροσβεστήρες ξηράς κόνεως.

Επιπλέον, κάθε εργαζόμενος οφείλει να:

- Διατηρεί το χώρο καθαρό
- Είναι σε εγρήγορση και να παρατηρεί οτιδήποτε ασυνήθιστο συμβαίνει στο χώρο και τις συσκευές
- Καθαρίζει αμέσως μετά τη χρήση όλες τις συσκευές και να μην αφήνει υπολείμματα
- Χρησιμοποιεί με ασφαλή τρόπο τις ηλεκτρικές συσκευές, όπως φούρνο μικροκυμάτων, τοστιέρα, ψυγείο κλπ.
- Απενεργοποιεί την ηλεκτρική συσκευή μετά τη χρήση της

2.5 Computer Room

Το Υπουργείο διαθέτει ειδικό χώρο για το Computer Room, όπου τηρούνται όλα τα μέτρα για τη διασφάλιση του εξοπλισμού και κατ' επέκταση της πληροφοριακής υποδομής.

- Η πρόσβαση στο Computer Room γίνεται μόνο από εξουσιοδοτημένα άτομα με ειδική σήμανση στην πόρτα, η οποία είναι κλειδωμένη.
- Για τα μη εξουσιοδοτημένα άτομα που εισέρχονται στο Computer Room, τηρείται βιβλίο εισόδου - εξόδου που περιλαμβάνει τα εξής:
    - ✓ Ονοματεπώνυμο επισκέπτη
    - ✓ Ονοματεπώνυμο συνοδού
    - ✓ Αιτιολογία εισόδου στον χώρο
    - ✓ Υπογραφή συνοδού
    - ✓ Υπογραφή επισκέπτη

Στην περίπτωση που μη εξουσιοδοτημένο άτομο εισέρχεται στον χώρο του Computer Room βρίσκεται πάντα υπό τη συνοδεία ατόμου/ατόμων που έχει δικαίωμα εξουσιοδοτημένης πρόσβασης στο χώρο.

Το βιβλίο εισόδου/εξόδου φυλάσσεται και επιθεωρείται από αρμόδιο άτομο της ΓΔΠΕ, στο τέλος κάθε εβδομάδας.

Επιπροσθέτως,

- Υφίστανται ανιχνευτές καπνού, αισθητήρες θερμοκρασίας και υγρασίας με ενδείξεις εκτός του χώρου του Computer Room και συστήματα πυρόσβεσης/πυροπροστασίας
- Λαμβάνονται όλα τα απαραίτητα μέτρα προκειμένου η θερμοκρασία του χώρου εντός των rack να κυμαίνεται στους 22 °C (+/-2 °C) και η υγρασία στο 45 % (+/- 5%)
- Απαγορεύεται η χρήση κινητών τηλεφώνων, ή άλλου εξοπλισμού που εκπέμπει ραδιοακτινοβολία μέσα στο χώρο του Computer Room
- Δεν επιτρέπεται η κατανάλωση φαγητού ή ποτού εντός του Computer Room

2.6 Χώροι αποθήκευσης φυσικού αρχείου και εξοπλισμού

Το έντυπο υλικό του αρχείου διατηρείται στο χώρο του κάθε Τμήματος ξεχωριστά, σύμφωνα με τα όσα ορίζονται στην Πολιτική Διατήρησης (βλ. Πολιτική Διατήρησης). Οι χώροι φύλαξης (γραφεία) καθώς και τα ντουλάπια φύλαξης του φυσικού αρχείου είναι κλειδωμένα.

Όταν ο εργαζόμενος απουσιάζει, τα έγγραφα για τα οποία είναι υπεύθυνος αποθηκεύονται πάντα σε κλειδωμένο συρτάρι ή ντουλάπι και δεν παραμένουν ποτέ σε κοινή θέα.
Οι εξυπηρετητές (servers), καθώς και ο τηλεπικοινωνιακός εξοπλισμός τοποθετούνται μόνο εντός του Computer Room του Υ.Μ.Α.. Αναφορικά με τον υπηρεσιακό εξοπλισμό που έχει χορηγηθεί σε εργαζομένους, υπεύθυνος για την ασφαλή φύλαξη του είναι ο ίδιος ο εργαζόμενος. Συσκευές που δεν χρησιμοποιούνται, φυλάσσονται προσωρινά σε ασφαλή διαμορφωμένο χώρο εντός του κτηρίου. Ο εξοπλισμός που δεν χρησιμοποιείται (π.χ. φωτοτυπικά, εκτυπωτές), φυλάσσεται μακριά από κοινή θέα.
Ο υπολογιστικός και τηλεπικοινωνιακός εξοπλισμός του Υ.Μ.Α. υπόκειται σε τακτική προληπτική συντήρηση είτε από τους προμηθευτές είτε από τους τεχνικούς του Υ.Μ.Α. σύμφωνα με τις οδηγίες των αντίστοιχων κατασκευαστών ή/ και προμηθευτών.

2.7 Γενικοί κανόνες για κεντρικές και περιφερειακές εγκαταστάσεις

Η φυσική ασφάλεια του Υ.Μ.Α διέπεται από τους ακόλουθους κανόνες:

- Ειδική φωτιζόμενη σήμανση αναρτάται σε όλες τις εξόδους κινδύνου των εγκαταστάσεων
- Η πρόσβαση στους χώρους που φυλάσσονται δεδομένα προσωπικού χαρακτήρα, είτε σε ψηφιακή, είτε σε φυσική μορφή, είναι περιορισμένη και επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα, καθώς οι πόρτες των αντίστοιχων χώρων παραμένουν κλειδωμένες
- Κάθε φορά που λύεται η σχέση εργασίας εργαζομένου, ανακαλούνται άμεσα τα δικαιώματα πρόσβασής του στις εγκαταστάσεις του Υπουργείου
- Η κατανάλωση φαγητού επιτρέπεται μόνο στο χώρο της κουζίνας και στα γραφεία με εξαίρεση των φαγητών σε υγρή μορφή (σούπες κτλ.)
- Κατανάλωση αφεψημάτων επιτρέπεται στο χώρο των γραφείων ή των διαδρόμων, εφόσον αποθηκεύονται σε συσκευασία που κλείνει
- Απαγορεύεται η ρίψη χαρτιού και γενικότερα οποιουδήποτε αντικειμένου στην τουαλέτα
- Απαγορεύεται το κάπνισμα σε όλους τους χώρους του Υ.Μ.Α.
- Ανά τακτά χρονικά διαστήματα πραγματοποιούνται καθαρισμοί και συντήρηση των κεντρικών και περιφερειακών κτηρίων του Υ.Μ.Α.

3. Πολιτική «Καθαρού Γραφείου» (Clean Desk) και «Καθαρής Οθόνης» (Clear Screen)

3.1 Ειδικές οδηγίες και κανόνες

Ο εργαζόμενος του Υ.Μ.Α. οφείλει να μεριμνά για την προστασία του εξοπλισμού που έχει στη διάθεσή του, ακόμα και κατά το χρονικό διάστημα που απουσιάζει από τη θέση εργασίας του ή τις εγκαταστάσεις του Υπουργείου. Για το σκοπό αυτό ακολουθούνται οι εξής βασικές αρχές:

- Τα κλειδιά που χρησιμοποιούνται για την πρόσβαση σε συρτάρια, ντουλάπια ή χώρους περιορισμένης πρόσβασης είναι διαρκώς υπό την κατοχή και επίβλεψη του αρμόδιου προσώπου
- Στην επιφάνεια εργασίας του υπολογιστή δεν αποθηκεύονται αρχεία με τίτλο στον οποίο να αναγράφονται προσωπικά δεδομένα π.χ. ονόματα αρχείων «Χρωστούμενα Παπαδόπουλος»

- Κατά την εκτύπωση εγγράφων που περιέχουν προσωπικά δεδομένα ή δεδομένα υψηλής σημασίας, αυτά παραλαμβάνονται άμεσα από τον εκτυπωτή
- Η προστασία οθόνης – οθόνη κλειδώματος είναι ενεργοποιημένη σε όλους τους υπολογιστές (κλείδωμα μέσα σε 20' λεπτά από την τελευταία ενέργεια του χρήστη). Η απενεργοποίηση της προστασίας οθόνης απαιτεί την εισαγωγή των διαπιστευτηρίων ασφάλειας του χρήστη (passwords)
- Απαγορεύεται η αναγραφή κωδικών ή άλλων δεδομένων προσωπικού χαρακτήρα σε χαρτάκια κολλημένα στην οθόνη ή άλλα μη προστατευμένα σημεία στο γραφείο των εργαζομένων
- Τα έγγραφα στα οποία αναγράφονται προσωπικά ή/και υπηρεσιακά δεδομένα, δεν πρέπει να βρίσκονται σε κοινή θέα
- Ο εργαζόμενος οφείλει να μεταφέρει στον καταστροφέα εγγράφων τα έγγραφα τα οποία δεν χρήζουν περαιτέρω επεξεργασίας και περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα προς ασφαλή καταστροφή
- Στο τέλος της εργάσιμης ημέρας, οι εργαζόμενοι πρέπει να φυλάσσουν σε ασφαλή σημεία (όπως χρηματοκιβώτια, πυρασφαλείς φωριαμούς, κλειδωμένα συρτάρια, ντουλάπια) όλα τα έγγραφα και τα αποσπώμενα ηλεκτρονικά μέσα (usb συσκευές αποθήκευσης μνήμης, εξωτερικοί σκληροί δίσκοι κλπ.) καθώς και τον φορητό εξοπλισμό (π.χ. laptops) που έχουν στη διάθεσή τους
- Ο εργαζόμενος οφείλει να είναι σε εγρήγορση και να ελέγχει τακτικά τον χώρο του και τον εξοπλισμό που του έχει διατεθεί. Συγκεκριμένα, οφείλει να:
  - Να διατηρεί σε καλή κατάσταση τον εξοπλισμό που του παρέχεται
  - Να ελέγχει το ασφαλές κλείδωμα των φωριαμών και συρταριών του
  - Να ελέγχει την ακεραιότητα του φυσικού αρχείου που είναι υπό την ευθύνη του
- Σε περίπτωση που διαπιστωθεί πρόβλημα στα ανωτέρω, οφείλει να ενημερώσει άμεσα την Ομάδα Αντιμετώπισης Περιστατικών Παραβίασης (cert@migration.gov.gr).
- Στην περίπτωση που ο εργαζόμενος αντιληφθεί πρόβλημα στον εργασιακό χώρο συναδέλφου, όπως ανοιχτά συρτάρια, ξεχασμένος ανοιχτός υπολογιστής κλπ., τότε σε πρώτη φάση, το αναφέρει στον συνάδελφο του, προκειμένου να λάβει τα απαραίτητα μέτρα. Εάν δε λάβει τα απαραίτητα προβλεπόμενα από την πολιτική μέτρα και υπάρχει επανάληψη παρόμοιων συμβάντων, ο εργαζόμενος οφείλει να ενημερώσει τον αρμόδιο προϊστάμενο
- Απαγορεύεται ο εργαζόμενος να χρησιμοποιεί το γραφείο συναδέλφου, όταν ο δεύτερος απουσιάζει, εκτός εάν έχει δοθεί η συγκατάθεση από τον δεύτερο ή/και από τον προϊστάμενο της οργανικής του μονάδας
- Σε περίπτωση εκκένωσης λόγω έκτακτης ανάγκης (συναγερμός, πυρκαγιά, κλπ.), εφόσον το επιτρέπει ο χρόνος και μόνο τότε, ο εργαζόμενος δύναται να διασφαλίσει όλα τα σημαντικά έγγραφα και τα ηλεκτρονικά μέσα

4. Πολιτική Εξουσιοδοτημένης Πρόσβασης

4.1 Διαβάθμιση ρόλων

Παρέχεται διαβαθμισμένη πρόσβαση σε διοικητικά στελέχη, εργαζομένους και προκαθορισμένους συνεργάτες του Υπουργείου, τόσο στους πληροφοριακούς πόρους, όσο

και στις φυσικές εγκαταστάσεις (γραφεία, αποθήκες, κ.τ.λ.). Η εν λόγω Πολιτική περιγράφει τις αρχές της διαβαθμισμένης πρόσβασης στους χώρους του Υπουργείου και στην πληροφοριακή υποδομή του, έχοντας ως γνώμονα τις εξής **γενικές αρχές διαβάθμισης ρόλων για τους χρήστες του Υπουργείου.**

- Τα δικαιώματα των χρηστών είναι ανάλογα του ρόλου τους και των ενεργειών που επιτελούν στους πληροφοριακούς πόρους
- Τα δικαιώματα πρόσβασης που έχει ο κάθε χρήστης σε συστήματα ή εφαρμογές του φορέα είναι επακριβώς ορισμένα και αυστηρά συνδεδεμένα με τις απαιτήσεις της εργασίας του, τις αρμοδιότητές του και τις συμβατικές του υποχρεώσεις, βάσει της θέσης εργασίας του και του τμήματος στο οποίο ανήκει ή προσφέρει τις υπηρεσίες του
- Τα δικαιώματα των χρηστών είναι ανάλογα της κρισιμότητας και του επιπέδου διαβάθμισης των πληροφοριών στις οποίες έχουν πρόσβαση
- Τα δικαιώματα των χρηστών επανεξετάζονται περιοδικά και προσαρμόζονται αναλόγως των απαιτήσεων
- Τα δικαιώματα των χρηστών επανεξετάζονται και εκτάκτως, κατόπιν εντολής της Διοίκησης του Υπουργείου ή πρωτοβουλίας του αρμοδίου υπαλλήλου της Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών
- Κάθε χρήστης συσχετίζεται με ένα μόνο προφίλ Χρήστη ανά πληροφοριακό σύστημα ή εφαρμογή
- Οι ομάδες χρηστών έχουν τα ελάχιστα δυνατά δικαιώματα που είναι απαραίτητα για την εκτέλεση των καθηκόντων τους
- Προνομιακά δικαιώματα πρόσβασης, π.χ. διαχειριστή, εκχωρούνται μόνο σε συγκεκριμένα πρόσωπα που είναι υπεύθυνα ανά σύστημα ή εφαρμογή και κατόπιν αιτιολογημένης πρότασης του αιτούντος ή με απόφαση της Διοίκησης. Η προνομιακή πρόσβαση περιορίζεται στο αναγκαίο χρονικό διάστημα
- Η ανάκληση των δικαιωμάτων πρόσβασης του χρήστη (πχ. σε περίπτωση διακοπής της συνεργασίας, αλλαγής ρόλου κ.λπ.) είναι άμεση και πραγματοποιείται από υπάλληλο της Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών σε συνεννόηση με τον προϊστάμενο του εκάστοτε αρμόδιου τμήματος
- Ειδικά όσον αφορά τα διαχειριστικά κέντρα των Π.Σ. και των υποδομών του Υπουργείου, τα δικαιώματα πρόσβασης δίνονται στους υπαλλήλους της ΓΔΠΕ κατόπιν εισηγήσεως του Τμήματος Ασφάλειας Πληροφοριών, Συστημάτων και Εφαρμογών προς τον προϊστάμενο της Διεύθυνσης Υποδομών Πληροφορικής &Επικοινωνιών και κατόπιν τελικής έγκρισης από τον προϊστάμενο της Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών.

4.2 Πρόσβαση στα δεδομένα και στους υλικοτεχνικούς πόρους του φορέα

Η διαβάθμιση των ρόλων των χρηστών και η πρόσβαση τους σε αυτά ορίζεται με γνώμονα την κατηγοριοποίηση των δεδομένων (προσωπικού χαρακτήρα και μη). Συγκεκριμένα, η πρόσβαση ορίζεται ως εξής:

Κατηγορία δεδομένων	Περιορισμός πρόσβασης
Δεδομένα Προσωπικού Χαρακτήρα	Η πρόσβαση σε πληροφορίες αυτής της κατηγορίας επιτρέπεται μόνο σε όσα στελέχη του Υπουργείου

	είναι απαραίτητα για την διεκπεραίωση των καθημερινών τους εργασιών.
Ευαίσθητα Δεδομένα Προσωπικού Χαρακτήρα	Η πρόσβαση σε πληροφορίες αυτής της κατηγορίας επιτρέπεται μόνο σε όσα στελέχη του Υπουργείου είναι απαραίτητα για την διεκπεραίωση των καθημερινών τους εργασιών.
Ενδοϋπηρεσιακά δεδομένα	Η πρόσβαση σε πληροφορίες αυτή της κατηγορίας επιτρέπεται μόνον σε εργαζομένους του Υπουργείου.
Εμπιστευτικά ενδοϋπηρεσιακά Δεδομένα	Η πρόσβαση σε πληροφορίες αυτής της κατηγορίας επιτρέπεται μόνο στα διοικητικά στελέχη, τους Γενικούς Διευθυντές, τους Διευθυντές και προϊσταμένους τμημάτων του Υπουργείου.
Δεδομένα δημόσιας χρήσης	Η πρόσβαση σε πληροφορίες αυτής της κατηγορίας επιτρέπεται σε όλους.

Η ταυτοποίηση και αυθεντικοποίηση των χρηστών στους σταθμούς εργασίας, στα Π.Σ. και στις Εφαρμογές του Υ.Μ.Α. γίνεται με τη χρήση σύγχρονων τεχνολογιών ισχυρής ταυτοποίησης (strong authentication), όπως μεθόδων ελέγχου ταυτότητας πολλαπλών παραγόντων.

4.3 Μέτρα που λαμβάνει ο εργαζόμενος

Τα απαραίτητα μέτρα που πρέπει να λαμβάνει ο κάθε εργαζόμενος είναι τα ακόλουθα:

- Να χρησιμοποιεί ισχυρούς κωδικούς πρόσβασης σύμφωνα με τα σχετικά πρότυπα (κυρίως άνω των οκτώ χαρακτήρων, συνδυασμός αλφαριθμητικών χαρακτήρων)
- Να μην χρησιμοποιεί εύκολα προβλέψιμους κωδικούς πρόσβασης (πχ. την ημερομηνία γέννησης του, το όνομά του κλπ.)
- Να τηρεί μυστικά τα στοιχεία του προσωπικού λογαριασμού του (όνομα χρήστη και κωδικός) και να ειδοποιεί άμεσα το cert@migration.gov.gr για τυχόν διαρροή τους
- Να μην κοινοποιεί σε κανέναν τρίτο (ούτε τηλεφωνικά ούτε με ηλεκτρονικό ταχυδρομείο) τους προσωπικούς κωδικούς πρόσβασης του
- Να μην σημειώνει τους κωδικούς του σε μέρη όπου μπορούν να αποκαλυφθούν εύκολα (π.χ. σε εκτεθειμένα χαρτιά ή αρχεία)
- Να μην κάνει χρήση του ίδιου συνθηματικού που χρησιμοποιείται σε λογαριασμούς του Υπουργείου για την πρόσβαση σε ηλεκτρονικές υπηρεσίες εκτός του Υπουργείου
- Να λαμβάνει μέριμνα, ώστε να αλλάζει τους κωδικούς ανά τακτά χρονικά διαστήματα
- Να κλειδώνει με μυστικό προσωπικό κωδικό την επιφάνεια εργασίας του υπολογιστή του όταν απουσιάζει από το γραφείο του
- Κατά την αλλαγή του κωδικού πρόσβασης, απαγορεύεται η χρήση των τελευταίων τριών (3) κωδικών που έχουν χρησιμοποιηθεί από τον χρήστη
- Να απενεργοποιεί τον Η/Υ κατά την αποχώρησή του από το γραφείο

4.4 Απόδοση και αφαίρεση δικαιωμάτων πρόσβασης

Η δημιουργία προφίλ κατά περίπτωση και η απόδοση των δικαιωμάτων πρόσβασης σε χρήστη ή ομάδα χρηστών γίνεται από το Αρμόδιο Τμήμα. Στους εργαζομένους αποδίδονται

τα δικαιώματα κατά την πρόσληψη με οποιονδήποτε τρόπο και σε συνεργάτες με την έναρξη της σύμβασης, βάσει της οποίας πρέπει να παραχωρηθούν δικαιώματα σε συνεργάτη.

Η αφαίρεση ή αναθεώρηση των δικαιωμάτων πραγματοποιείται από το Αρμόδιο Τμήμα για λόγους εκούσιας ή ακούσιας αποχώρησης του προσωπικού, λήξης της σύμβασης, για λόγους μετάθεσης ή μετακίνησης σε άλλο τομέα εργασίας, είτε για λόγους αλλαγής των αναγκών που υπάρχουν βάσει σύμβασης και γενικότερα εξωγενών παραγόντων, που πιθανώς επηρεάζουν τη λειτουργία του Υπουργείου. Επιπρόσθετα, η αφαίρεση ή η αναθεώρηση των δικαιωμάτων μπορεί να συμβεί με απόφαση της Διοίκησης γενικότερα ή κατόπιν εντοπισμού κάποιου περιστατικού, σύμφωνα και με τα ειδικότερα που προβλέπονται στο Σχέδιο Διαχείρισης Συμβάντων του Υπουργείου.

Σε περίπτωση που κριθεί αναγκαία η εκχώρηση ή η μεταβολή της πρόσβασης κάποιου χρήστη σύμφωνα με τα παραπάνω, τότε θα πρέπει να υποβάλλεται εγγράφως σχετικό αίτημα στο Αρμόδιο Τμήμα (π.χ. μέσω συστήματος Υποστήριξης Υπηρεσιών Πληροφορικής – ΑΤΛΑΣ), το οποίο θα συνοδεύεται και από την έγκριση του αρμόδιου προϊσταμένου.

5.Πολιτική Κωδικών Πρόσβασης

5.1 Ειδικές οδηγίες και κανόνες

Όλοι οι κωδικοί (passwords) των συστημάτων/εφαρμογών να αλλάζουν σε τακτική βάση (3-9 μήνες). Για την αλλαγή του password ο χρήστης ενημερώνεται με αυτοματοποιημένο μήνυμα.

Οι κωδικοί (passwords) δεν πρέπει να διακινούνται μέσω ηλεκτρονικών μηνυμάτων ή άλλων μέσων ηλεκτρονικής επικοινωνίας ανάμεσα στους χρήστες.

Παρακάτω ακολουθεί μία λίστα από ενέργειες που πρέπει να αποφευχθούν:

- Να μην χρησιμοποιείται ο ίδιος κωδικός (password) για λογαριασμούς που χρησιμοποιούνται εντός του φορέα και για τους προσωπικούς λογαριασμούς των υπαλλήλων
- Να μην χρησιμοποιούνται εύκολα προβλέψιμοι κωδικοί πρόσβασης (πχ. η ημερομηνία γέννησης, το όνομα κλπ.)
- Όπου είναι δυνατό, να μην χρησιμοποιείται ο ίδιος κωδικός (password) για διαφορετικές ανάγκες πρόσβασης
- Να μην κοινοποιούνται οι προσωπικοί κωδικοί (passwords) πρόσβασης των εφαρμογών και των συστημάτων του Υπουργείου σε κανέναν, συμπεριλαμβανομένου και των βοηθών διαχείρισης ή γραμματέων
- Οι αρμόδιοι διαχειριστές της Γ.Δ. Πληροφορικής και Επικοινωνιών δεν πρόκειται ποτέ να ζητήσουν τους προσωπικούς κωδικούς πρόσβασης των υπαλλήλων
- Να μην αποκαλύπτονται οι κωδικοί (passwords) μέσω τηλεφώνου σε κανέναν
- Να μην αποκαλύπτονται οι κωδικοί (passwords) με ηλεκτρονικό μήνυμα σε κανέναν
- Στους κωδικούς πρόσβασης εφαρμόζεται το κριτήριο της πολυπλοκότητας (ελάχιστο μήκος κωδικού, χρήση αριθμών και συμβόλων, χρήση πεζών και κεφαλαίων γραμμάτων), όπως αυτό προσδιορίζεται σε κάθε Π.Σ. και εφαρμογή του Υ.Μ.Α.

Σε περίπτωση απώλειας κωδικών πρόσβασης, ο εργαζόμενος θα πρέπει να απευθύνει αίτημα αρχικοποίησης στο Σύστημα Υποστήριξης Υπηρεσιών Πληροφορικής – ΑΤΛΑΣ. Οι προσωρινοί κωδικοί πρόσβασης στα συστήματα εφαρμογών και υποδομών του Υ.Μ.Α. γνωστοποιούνται

είτε δια ζώσης είτε τηλεφωνικώς στον ενδιαφερόμενο με τη συμπληρωματική χρήση τουλάχιστον δύο ερωτήσεων ταυτοποίησης.

6.Πολιτική Απομακρυσμένης Πρόσβασης

6.1 Ειδικές οδηγίες και κανόνες

Σε περίπτωση που κριθεί απαραίτητη η δυνατότητα απομακρυσμένης πρόσβασης στα συστήματα του Υπουργείου, τηρούνται συγκεκριμένοι κανόνες.

- Η πραγματοποίηση απομακρυσμένης πρόσβασης πραγματοποιείται μόνο από εξουσιοδοτημένα άτομα (Παράρτημα Ι)
- Τα δεδομένα προσωπικού χαρακτήρα που αποθηκεύονται τοπικά είναι τα ελάχιστα για την εκπλήρωση της εργασίας
- Στους υπολογιστές είναι εγκατεστημένο και ενημερωμένο όλο το απαραίτητο λογισμικό (όπως antivirus, firewalls, κλπ.) και οι ρυθμίσεις ασφάλειας που απαγορεύουν την εγκατάσταση επιπλέον προγραμμάτων
- Αν η πρόσβαση παραχωρείται σε εξωτερικό συνεργάτη στα πλαίσια της σύμβασής του, τότε δίνει εγγράφως τις εγγυήσεις για όλα τα παραπάνω
- Κατά τη διάρκεια της χρήσης του, ο υπολογιστής είναι συνεχώς υπό την επιτήρηση του χρήστη
- Απαγορεύεται η εγκατάσταση οποιουδήποτε συστήματος απομακρυσμένης πρόσβασης σε συστήματα του φορέα από μη εξουσιοδοτημένα άτομα
- Η δυνατότητα απομακρυσμένης πρόσβασης σε συστήματα του φορέα, δίνεται μόνο όταν υπάρχει τεκμηριωμένη ανάγκη και μόνο για όσα συστήματα και για όση χρονική διάρκεια απαιτείται
- Οι διαδικασίες απομακρυσμένης πρόσβασης του Υπουργείου γίνονται αποκλειστικά μέσω Virtual Private Network (VPN)
    - Η διαχείριση των πυλών του VPN πραγματοποιείται από το αρμόδιο τμήμα
    - Όλοι οι υπολογιστές, οι οποίοι συνδέονται στο εσωτερικό δίκτυο του Υπουργείου μέσω VPN χρησιμοποιούν ενημερωμένο λογισμικό antivirus
    - Οι χρήστες του VPN αποσυνδέονται αυτόματα από το δίκτυο του Υπουργείου μετά από τριάντα λεπτά μη ενεργούς δράσης. Ο χρήστης θα πρέπει να ξανασυνδεθεί στο δίκτυο
    - Αν πραγματοποιηθεί χρήση της VPN τεχνολογίας με προσωπικό εξοπλισμό, στις περιπτώσεις που αυτό επιτρέπεται βάσει της παρούσας, οι χρήστες θα πρέπει να γνωρίζουν, ότι τα μηχανήματα τους είναι η προέκταση του δικτύου του φορέα, και υπόκεινται στο σύνολο των πολιτικών και διαδικασιών του

7. Πολιτική Ορθής Χρήσης Υπηρεσιακών Συσκευών και Εξοπλισμού

7.1 Υποχρεώσεις εργαζομένου :

Ο εργαζόμενος οφείλει να τηρεί κάποιους κανόνες για να διασφαλίζει την ορθή και ασφαλή λειτουργία των υπηρεσιακών συσκευών και εξοπλισμού.

Ειδικότερα:

- Η χρήση των συσκευών και του εξοπλισμού πραγματοποιείται αυστηρά στα πλαίσια της εργασίας και των καθηκόντων του υπαλλήλου
- Απαγορεύεται η αποθήκευση προσωπικών δεδομένων (ευαίσθητων και μη) στην υπηρεσιακή συσκευή και αντιστρόφως
- Οι οθόνες των υπηρεσιακών συσκευών-ηλεκτρονικών υπολογιστών δεν πρέπει να είναι ορατές σε μη εξουσιοδοτημένους χρήστες κατά τη χρήση αυτών σε χώρο εκτός του Υπουργείου
- Η τήρηση των οδηγιών αναφορικά με τους κωδικούς πρόσβασης (Βλ. Οδηγίες Κωδικών πρόσβασης)
- Να μην χρησιμοποιείται η υπηρεσιακή συσκευή από τρίτους, εκτός εάν δημιουργηθούν διαφορετικά προφίλ εισόδου για κάθε χρήστη ξεχωριστά κατόπιν έγκρισης της διοίκησης του Υπουργείου
- Στην περίπτωση βλάβης/κλοπής/απώλειας της συσκευής, ο εργαζόμενος οφείλει να ενημερώσει αμελλητί την Ομάδα Αντιμετώπισης Περιστατικών Παραβίασης (CERT): cert@migration.gov.gr
- Σε περίπτωση λύσης της σύμβασης εργασίας με οποιονδήποτε τρόπο (καταγγελία, οικειοθελής αποχώρηση, λύση λόγω παρόδου του συμβατικού χρόνου κ.λπ.) υποχρεούται να παραδώσει την υπηρεσιακή συσκευή, όπως ακριβώς την παρέλαβε
- Ο εργαζόμενος απαγορεύεται να τροποποιεί τις ρυθμίσεις του υπηρεσιακού υπολογιστή
- Τα laptops μεταφέρονται πάντα μέσω ειδικής τσάντας μεταφοράς για την προστασία τους από φθορές
- Ο εξοπλισμός επιστρέφεται πάντα στο Υπουργείο σε καλή και λειτουργική κατάσταση χωρίς βλάβες και ζημιές
- Απαγορεύεται η σύνδεση δικτυακού εξοπλισμού στις πρίζες του δικτύου δεδομένων, πλην αυτού που παρέχεται
- Κανένας χρήστης δεν δύναται να αλλάξει IP διεύθυνση υπολογιστή, κάρτα δικτύου, ή πρίζα
- Οι χρήστες των πληροφοριακών πόρων του ΥΜΑ δεν επιτρέπεται να εγκαθιστούν προγράμματα λογισμικού πέρα από αυτά που είναι προδιαγραμμένα για κάθε υπολογιστική μονάδα ανάλογα με το ρόλο του χρήστη
- Οι υπεύθυνοι για την εγκατάσταση προγραμμάτων λογισμικού είναι μόνο οι διαχειριστές των συστημάτων
- Δεν επιτρέπεται η σύνδεση εξωτερικών αποθηκευτικών μέσων στις υπολογιστικές μονάδες των χρηστών, εκτός των περιπτώσεων που απαιτείται από τη φύση της εργασίας του υπαλλήλου και μόνο κατόπιν έγκρισης από δύο ανωτέρους του, Προϊσταμένους και τελική ενυπόγραφη έγκριση από το αρμόδιο τμήμα της Γ.Δ. Πληροφορικής και Επικοινωνιών
- Δεν επιτρέπεται το «άνοιγμα» εκτελέσιμων αρχείων από εξωτερικά αποθηκευτικά μέσα που συνδέονται στις υπολογιστικές μονάδες των χρηστών
- Δεν επιτρέπεται το «άνοιγμα» εκτελέσιμων αρχείων που επισυνάπτονται σε email
- Δεν επιτρέπεται η χρήση εφαρμογών (ftp, p2p κ.α.) με τις οποίες δύναται ο χρήστης να μεταφέρει αρχεία από δικτυακούς τόπους στην υπολογιστική του μονάδα εκτός των περιπτώσεων που απαιτείται από τον χαρακτήρα της εργασίας του υπαλλήλου και έχει δοθεί σχετική άδεια από το αρμόδιο τμήμα Ασφάλειας Πληροφοριών, Συστημάτων και Εφαρμογών

- Οι χρήστες οφείλουν να συνεργάζονται με τους διαχειριστές συστημάτων προκειμένου να διερευνάται η εγκατάσταση κακόβουλου λογισμικού σε περίπτωση ανίχνευσής του στις υπολογιστικές τους μονάδες
- Οι χρήστες δεν επιτρέπεται να χρησιμοποιούν το λογισμικό που τους παρέχεται για την πρόσβαση σε πληροφορίες και συστήματα για τα οποία δεν έχουν λάβει την απαραίτητη εξουσιοδότηση
- Οι χρήστες δεν επιτρέπεται να χρησιμοποιούν το λογισμικό που τους παρέχεται για μεταφορά δεδομένων και γενικότερα στοιχείων που αποτελούν περιουσιακό στοιχείο του Υ.Μ.Α εκτός των ορίων του Υπουργείου και εκτός των συστημάτων του, χωρίς προηγούμενη έγκριση του Προϊσταμένου του οικείου τμήματος
- Δεν επιτρέπεται η χρήση των υπολογιστικών μονάδων για πρόσβαση, επεξεργασία και διακίνηση υλικού με ρατσιστικό, πορνογραφικό ή οποιουδήποτε άλλου παράνομου, μη αποδεκτού και επιβλαβούς περιεχομένου
- Οι προσφερόμενες υπηρεσίες, τα μέσα και οι υποδομές του Υπουργείου όπως ηλεκτρονική αλληλογραφία (e-mail), πρόσβαση στο διαδίκτυο, φορητά υπολογιστικά μέσα κ.λπ. διατίθενται για χρήση μόνο στα πλαίσια της εργασίας
- Οι χρήστες δεν επιτρέπεται να προβαίνουν σε καμία ενέργεια παραβίασης των πολιτικών που καθορίζουν την πρόσβαση σε ιστοχώρους του διαδικτύου και εφαρμόζονται στα συστήματα ασφάλειας του Υπουργείου
- Απαγορεύεται η εγκατάσταση λογισμικού ή δεδομένων χωρίς άδεια, στα συστήματα των χρηστών
- Τα αρχεία MP3/MP4 ή άλλου είδους αρχεία μουσικής/βίντεο, απαγορεύονται εκτός εάν οι χρήστες κατέχουν νόμιμη άδεια για τα συγκεκριμένα αρχεία.
- Σε όλους τους Η/Υ (σταθμοί εργασίας & φορητοί υπολογιστές) χρησιμοποιείται προστασία οθόνης (Screen Saver) με κωδικό πρόσβασης, με αυτόματο χρόνο αναμονής 10 λεπτά ή λιγότερο
- Όλα τα μηχανήματα που περιλαμβάνουν εμπιστευτικές ή απόρρητες πληροφορίες, πρέπει να έχουν ενεργοποιημένη την εντολή εισαγωγής κωδικού πρόσβασης κατά την εκκίνησή τους (π.χ. BIOS).
- Οι χρήστες απενεργοποιούν (shutdown) τα μηχανήματα τα οποία χρησιμοποιούν (σταθμοί εργασίας, φορητοί υπολογιστές) μετά το πέρας της εργασίας τους ή όταν τα μηχανήματα παραμένουν ανεπιτήρητα για παρατεταμένο χρονικό διάστημα
- Οι χρήστες τερματίζουν τις ενεργές εφαρμογές μετά τη λήξη της εργασίας τους, εκτός αν αυτές μπορούν να πραγματοποιήσουν ασφαλή τερματισμό (π.χ. Screen Saver προστατευμένο με κωδικό πρόσβασης)

7.2 Έλεγχος συσκευών και ενέργειες από τον Οργανισμό

Το Υπουργείο διατηρεί το δικαίωμα:

- Να περιορίσει την πρόσβαση σε συγκεκριμένες συσκευές, οι οποίες συνδέονται είτε ασύρματα είτε ενσύρματα ή και με τους δύο τρόπους στο υπηρεσιακό δίκτυο
- Να περιορίσει την πρόσβαση σε συγκεκριμένες εφαρμογές
- Να λάβει όλα τα απαραίτητα μέτρα ανάκτησης πληροφοριών από τις συσκευές, οι οποίες ανήκουν στο Υ.Μ.Α.

Κατά την παράδοση των συσκευών στους εργαζομένους έχουν ληφθεί όλα τα απαραίτητα μέτρα προστασίας, στα οποία περιλαμβάνονται:

- Το αυτόματο κλείδωμα της συσκευής μετά από ορισμένο χρονικό διάστημα αδράνειας (ενδέχεται να διαφέρει ανάλογα την οργανική μονάδα του χρήστη)
- Η συσκευή ελέγχεται πριν τη παράδοση στον εργαζόμενο, αλλά και αμέσως μετά την επιστροφή της.
- Πραγματοποιείται εγκατάσταση αντιιϊκών προγραμμάτων
- Πραγματοποιείται εγκατάσταση μόνο των αναγκαίων για επιχειρησιακούς σκοπούς εφαρμογών και προγραμμάτων
- Διαγράφονται προσωπικά, υπηρεσιακά δεδομένα, εφαρμογές και προγράμματα που δεν είναι αναγκαία για τους σκοπούς εργασίας του υπαλλήλου
- Τηρείται μητρώο παράδοσης-επιστροφής συσκευών (χρεωστικό) με καταγραφή όλων των απαραίτητων στοιχείων σε φυσική και ηλεκτρονική μορφή

8.Πολιτική Ασφαλούς Χρήσης Ηλεκτρονικού Ταχυδρομείου

8.1 Ειδικοί κανόνες και οδηγίες

Η πιθανότητα εκτέλεσης κακόβουλων λογισμικών αυξάνεται στις συσκευές που συνδέονται στο διαδίκτυο, καθιστώντας το εσωτερικό δίκτυο του Υ.Μ.Α. ευάλωτο. Επομένως, απαγορεύεται οποιαδήποτε χρήση του διαδικτύου η οποία δύναται να θέσει σε κίνδυνο τα συμφέροντα του Υ.Μ.Α. Η σύνδεση των συσκευών στο διαδίκτυο ελέγχεται συνεχώς για ενδεχόμενη παραβίαση των δεδομένων. Επιπρόσθετα, η χρήση του ηλεκτρονικού ταχυδρομείου απαιτεί ιδιαίτερη προσοχή λόγω της επεξεργασίας προσωπικών και κρίσιμων υπηρεσιακών δεδομένων που πραγματοποιούνται μέσω αυτού. Επομένως, οι εργαζόμενοι τηρούν τους κάτωθι κανόνες:

Ηλεκτρονικό ταχυδρομείο email :

- Ιδιαίτερη προσοχή σε ύποπτα email. Πιο συγκεκριμένα, προηγείται ενδελεχής έλεγχος του ονόματος του αποστολέα και αποφεύγεται το κατέβασμα ή άνοιγμα αρχείων (με επεκτάσεις όπως .zip, 7z, .rar, .pif, .com, .bat, .exe, .vbs, και .lnk) για τα οποία ο χρήστης δεν είναι απολύτως σίγουρος για την ασφάλεια τους
- Τα αρχεία που είναι συνημμένα σε email δεν ανοίγονται εάν υπάρχει οποιαδήποτε αμφιβολία για την ταυτότητα του αποστολέα, καθότι υπάρχει κίνδυνος εγκατάστασης κακόβουλου λογισμικού (virus, Trojan horse, worms, spyware, toolkits) στους υπολογιστές και κατ' επέκταση μέσω του δικτύου σε όλα τα συστήματα του ΥΜΑ. Σε περίπτωση που το email φαίνεται ύποπτο (αρκετά ορθογραφικά ή/ και συντακτικά λάθη, κείμενο εκφοβισμού κ.λπ.), οι χρήστες επικοινωνούν με το αρμόδιο τμήμα Ασφάλειας Πληροφοριών, Συστημάτων και Εφαρμογών
- Σε περίπτωση που υπάρχει υποψία ότι ένα email περιέχει ιό, ενημερώνεται άμεσα το τμήμα Ασφάλειας Πληροφοριών, Συστημάτων και Εφαρμογών (cert@migration.gov.gr).
- Δεν επιτρέπεται χρήση του υπηρεσιακού ηλεκτρονικού ταχυδρομείου με τρόπο προσβλητικό για το Υ.Μ.Α.

- Δεν επιτρέπεται η διακίνηση ηλεκτρονικών μηνυμάτων για πρόσβαση, επεξεργασία και διακίνηση υλικού με ρατσιστικό, πορνογραφικό ή οποιουδήποτε άλλου παράνομου, μη αποδεκτού και επιβλαβούς περιεχομένου
- Δεν επιτρέπεται η διακίνηση ηλεκτρονικών μηνυμάτων με κακόβουλο/ιομορφικό λογισμικό
- Τηρούνται οι οδηγίες αναφορικά με τους κωδικούς πρόσβασης (Βλ. Οδηγίες Κωδικών πρόσβασης)
- Δεν επιτρέπεται η αποστολή σε άλλους χρήστες, ανεπιθύμητων ηλεκτρονικών μηνυμάτων (junk emails) ή άλλου διαφημιστικού ή προωθητικού περιεχομένου (spams)
- Τα συνημμένα αρχεία ηλεκτρονικής αλληλογραφίας που περιέχουν κρίσιμα υπηρεσιακά δεδομένα, προσωπικά δεδομένα και δεδομένα ειδικών κατηγοριών, κρυπτογραφούνται με λογισμικό ασύμμετρης κρυπτογράφησης (Kleopatra)
- Η χρήση του υπηρεσιακού λογαριασμού ηλεκτρονικής αλληλογραφίας για προσωπική χρήση απαγορεύεται.
- Δεν επιτρέπεται η κοινοποίηση (cc, bcc) σε χρήστες που δεν είναι εξουσιοδοτημένοι να έχουν πρόσβαση στις πληροφορίες που φέρει η ηλεκτρονική αλληλογραφία
- Διαγράφονται άμεσα τα email από δήθεν παρόχους οικονομικών υπηρεσιών (π.χ. Τράπεζες) με τα οποία ζητούνται τα συνθηματικά χρηστών ή οποιοδήποτε άλλο προσωπικό στοιχείο και γίνεται ειδοποίηση του τμήματος Ασφάλειας Πληροφοριών, Συστημάτων και Εφαρμογών
- Οι χρήστες λαμβάνουν ενημέρωση για ιούς ή κενά ασφαλείας μόνο από τη Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών
- Δεν πρέπει να αποκαλύπτεται σε καμία περίπτωση αναγνωριστικό (username – password) ηλεκτρονικών λογαριασμών
- Δεν πρέπει να αποστέλλονται μεγάλου μεγέθους αρχεία (πχ. video ή εικόνες) μέσω του ηλεκτρονικού ταχυδρομείου, καθώς δημιουργείται συμφόρηση και καθυστέρηση στο δίκτυο
- Δεν θα πρέπει να γνωστοποιείται η διεύθυνση ηλεκτρονικού ταχυδρομείου του εργαζόμενου του ΥΜΑ σε εξωτερικούς παρόχους ηλεκτρονικών υπηρεσιών ή σελίδες κοινωνικής δικτύωσης, e-shops, κ.λπ.
- Υπενθυμίζεται ότι το email (mailbox) δεν είναι αποθηκευτικός χώρος. Κάθε εργαζόμενος θα πρέπει να διενεργεί τακτική εκκαθάριση του ηλεκτρονικού ταχυδρομείου του.

9. Πολιτική Ασφαλούς Χρήσης Internet

9.1 Ειδικοί κανόνες και οδηγίες

- Η χρήση των Π.Σ. και εφαρμογών του Υ.Μ.Α, γίνεται αποκλειστικά για υπηρεσιακούς σκοπούς. Όλα τα δεδομένα που υπόκεινται σε επεξεργασία μέσω των άνωθεν εφαρμογών είναι υπηρεσιακά και όχι προσωπικά δεδομένα των χρηστών
- Απαγορεύεται η περιήγηση σε μη ασφαλείς διαδικτυακές τοποθεσίες (π.χ. σε αυτές που υπάρχει η σήμανση «μη ασφαλής» δίπλα από το URL, ή αλλιώς η έλλειψη πρωτοκόλλου https)
- Πραγματοποιείται σύνδεση μόνο σε ασφαλή δίκτυα με την υπηρεσιακή συσκευή (π.χ. δεν συνδεόμαστε σε ελεύθερο Wi-Fi που δεν υπάρχει κωδικός πρόσβασης)

- Τηρούνται όλες οι οδηγίες αναφορικά με τους κωδικούς πρόσβασης (Βλ. Οδηγίες Κωδικών πρόσβασης)
- Δεν επιτρέπεται η πρόσβαση σε δικτυακούς τόπους που θεωρούνται ακατάλληλοι για το χώρο εργασίας
- Δεν επιτρέπεται η πρόσβαση σε ρατσιστικό, πορνογραφικό ή οποιουδήποτε άλλο παράνομο, μη αποδεκτό και επιβλαβές περιεχόμενο.
- Απαγορεύεται να αναρτώνται φωτογραφίες ή προσωπικές πληροφορίες εργαζομένων συναδέλφων και εν γένει φυσικών προσώπων χωρίς την προηγούμενη ενημέρωση και συγκατάθεση αυτών.

Το διαδίκτυο (Internet) ΔΕΝ πρέπει να χρησιμοποιείται για:

- Αντιγραφή, αποκάλυψη, μεταφορά, αλλαγή ονομασίας, ανάγνωση ή διαγραφή πληροφοριών ή προγραμμάτων που ανήκουν σε άλλον χρήστη, χωρίς την έγκρισή του
- Αντιγραφή, αποκάλυψη, μεταφορά, αλλαγή ονομασίας, ανάγνωση ή διαγραφή πληροφοριών ή προγραμμάτων που ανήκουν στο ΥΜΑ, χωρίς προηγούμενη έγκριση από τα αρμόδια στελέχη του ΥΜΑ
- Παραβίαση ή παράκαμψη των μηχανισμών ασφαλείας που εφαρμόζει το ΥΜΑ για προστασία από τους κινδύνους του Internet
- Παράνομη πρόσβαση σε άλλο υπολογιστικό σύστημα ή υπηρεσία
- Κοινοποίηση λογαριασμών (accounts) ή κωδικών (passwords) άλλων χρηστών
- Άνοιγμα κάθε είδους αρχείου προερχόμενου από το Internet χωρίς να έχει προηγηθεί σάρωση από λογισμικό antivirus
- Δημιουργία λογαριασμών σε Online υπηρεσίες ή/ και κοινωνικά μέσα δικτύωσης (social media) όπως gmail, facebook κ.λπ. με ίδιο user name ή / και password που χρησιμοποιείται για πρόσβαση σε πληροφοριακούς πόρους του Υπουργείου (υπολογιστές, laptops, servers κ.α.)
- Αντιγραφή αρχείων μη επαγγελματικού περιεχομένου (downloading)

10. Πολιτική Ασφάλειας Δικτύου

10.1 Ειδικές οδηγίες και κανόνες

- Η παροχή δικτύωσης προς τους χρήστες των υπολογιστικών συστημάτων γίνεται με ενσύρματο τρόπο, ο οποίος εξασφαλίζει σε ικανοποιητικό βαθμό τη μη παρείσδυση εξωτερικών παραγόντων στο δίκτυο της υπηρεσίας
- Η προστασία από εξωγενείς απειλές διασφαλίζεται μέσω της χρήσης αντιικού λογισμικού - Antivirus
- Η επικοινωνία των workstation και των εφαρμογών με το διαδίκτυο ελέγχεται μέσω «Firewall» για εσωτερικά και εξωτερικά αιτήματα με άλλες διαδικτυακές υπηρεσίες και παρέχει λειτουργίες, όπως web filtering, application filtering, content filtering και anti-spam
- Σε ορισμένα σημεία κατ'εξαιρεση εφαρμογές όπως Χαρτογράφηση Κυκλοφορίας Αλλοδαπών (Αλκυόνη), φιλοξενούνται στο δίκτυο POL (Police –Online) της ΕΛ.ΑΣ.
- Το δίκτυο είναι σχεδιασμένο βάσει προτύπων τεχνολογίας καταλόγου χρηστών Active Directory και οι χρήστες πιστοποιούνται στο εσωτερικό δίκτυο από το κεντρικό σύστημα Windows Domain Controller. Η επικοινωνία μεταξύ των δικτυακών μερών γίνεται

διαβαθμισμένα και η πρόσβαση στους κεντρικούς Domain Controllers είναι απόλυτη, περιορισμένη και πλήρως ελεγχόμενη

- Η χρήση του ηλεκτρονικού ταχυδρομείου, του διαδικτύου και του κοινόχρηστου χώρου αποθήκευσης υλοποιείται σε ελεγχόμενο ασφαλές περιβάλλον με ελεγχόμενη πρόσβαση, ώστε να μην εκτίθενται σε κινδύνους τα δεδομένα που επεξεργάζεται το Υπουργείο
- Το δίκτυο προστατεύεται τόσο από εσωτερικές, όσο και από εξωτερικές απειλές μέσω ειδικών κανόνων ασφάλειας του τείχους προστασίας, ώστε να καθίσταται δυνατή η ανίχνευση, αλλά και αποτροπή κακόβουλων επιθέσεων
- Οι κανόνες του τείχους προστασίας με τις υπηρεσίες του Antivirus και της δυνατότητας παραμετροποίησης του Firewall λειτουργούν συνδυαστικά για την ανίχνευση και αποτροπή κακόβουλων επιθέσεων στο εσωτερικό δίκτυο του Υπουργείου
- Υφίσταται τεχνολογία IPS (Intrusion Prevention Systems) και IDS (Intrusion Detection Systems) για την ανίχνευση και προστασία του εσωτερικού δικτύου
- Χρησιμοποιείται τεχνολογία αποτροπής απώλειας δεδομένων (DLP) με κατάλληλη παραμετροποίηση για την αποτροπή διαρροής κοινόχρηστων πληροφοριών στην εφαρμογή Office 365
- Εντοπίζονται και αποκλείονται διευθύνσεις ιστοσελίδων και υπηρεσίες που κρίνονται ως υψηλού κινδύνου
- Κατά περίπτωση πραγματοποιούνται δοκιμές ελέγχου για την ασφάλεια των κρίσιμων συστημάτων και υποδομών (π.χ. Penetration Testing)

11. Πολιτική Bring Your Own Device (BYOD)

11.1 Ειδικές οδηγίες και κανόνες

Στους εργαζόμενους του Υπουργείου επιτρέπεται η χρήση προσωπικών συσκευών με τις οποίες μπορούν να συνδέονται στο δίκτυο και να επεξεργάζονται υπηρεσιακά δεδομένα. Επισημαίνεται δε ότι η εν λόγω χρήση προσωπικών συσκευών προϋποθέτει την κατάλληλη παραμετροποίηση και καταγραφή τους από τη Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών. Οι συγκεκριμένοι κανόνες σκοπό έχουν την ασφαλή χρήση αυτών των συσκευών.

Είδη συσκευών :

Η συγκεκριμένη Πολιτική καλύπτει τη χρήση μη υπηρεσιακών ηλεκτρονικών συσκευών που δύναται να έχουν οι εργαζόμενοι βάσει του πίνακα που ακολουθεί.

Συσκευές	Χρήση
smartphones, smartwatches	Υπηρεσίες ηλ. αλληλογραφίας και OneDrive
usb φορητές συσκευές	Χρήση μόνο για την εξυπηρέτηση ειδικών- έκτακτων αναγκών (πχ. τεχνικό πρόβλημα με υπηρεσίες OneDrive, προσωρινή αποθήκευση αρχείων)
Tablet, φορητοί υπολογιστές	Κάλυψη ειδικών αναγκών, σε ειδικές περιπτώσεις (πχ. συναντήσεις στελεχών, βλάβη τερματικού σταθμού)

11.2 Μέτρα για την ορθή χρήση προσωπικών συσκευών

Για να διασφαλιστεί η υπηρεσιακή υποδομή και τα υπηρεσιακά δεδομένα χρηστών, λαμβάνονται μέτρα και τίθενται αυστηροί κανόνες για την ορθή χρήση των προσωπικών συσκευών.

- Οι εργαζόμενοι ενημερώνονται για την σωστή χρήση των συσκευών μέσω των οδηγιών της Υπηρεσίας
- Οι εξωτερικοί συνεργάτες ή/και τρίτοι δεν επιτρέπεται να χρησιμοποιούν προσωπικές συσκευές για τη σύνδεση στο εσωτερικό δίκτυο (χωρίς προηγούμενη παραμετροποίησή τους από τη ΓΔΠΕ)
- Το περιεχόμενο των προσωπικών συσκευών των εργαζομένων κατά κανόνα δεν παρακολουθείται. Σε εξαιρετικές περιπτώσεις, όπως όταν υπάρχουν ενδείξεις κακόβουλης δραστηριότητας από εργαζόμενο ή συσκευής αποδεδειγμένα παραβιασμένης από κακόβουλο λογισμικό, το Υπουργείο ενδέχεται να προβεί σε ενέργειες παρακολούθησης της συσκευής σε επίπεδο που μπορεί να επηρεάσει την ιδιωτικότητα των εργαζομένων καταγράφοντας όλη τη δραστηριότητα της συσκευής
- Τηρείται μητρώο για κάθε εργαζόμενο ο οποίος χρησιμοποιεί προσωπική συσκευή. Το μητρώο συμπληρώνεται μέσω φόρμας από τον εργαζόμενο διαδικτυακά
- Μέσω του τμήματος υποστήριξης (support) αντιμετωπίζονται προβλήματα προσωπικών συσκευών εργαζομένων, εάν και εφόσον συνδέονται ή πρόκειται να συνδεθούν με το πληροφοριακό σύστημα του Υπουργείου (guest δίκτυο). Επίσης, λαμβάνονται μέτρα ώστε η εκάστοτε προσωπική συσκευή να μην βλάψει τις υποδομές του Υπουργείου. Σε περιπτώσεις που η υποστήριξη της προσωπικής συσκευής απαιτεί επιβάρυνση σε χρόνο από την εργασία ή οικονομική επιβάρυνση του Υπουργείου, παύει να χρησιμοποιείται ή ο ίδιος ο κάτοχος προβαίνει στην επίλυση του προβλήματος (π.χ. αντικατάσταση οθόνης tablet λόγω ζημίας)

11.3 Υποχρεώσεις των εργαζομένων

Ο εργαζόμενος οφείλει να τηρεί τους κανόνες ασφάλειας των προσωπικών του συσκευών (μετά την παραμετροποίησή τους από τη ΓΔΠΕ). Ανάλογα με το είδος της συσκευής, ο κάτοχός της είναι υπεύθυνος για την ασφάλειά της και οφείλει να τηρεί τα ακόλουθα μέτρα προστασίας:

- Αφαιρούνται τα αποσπώμενα αποθηκευτικά μέσα (usb) με ασφαλή κατάργηση
- Χρησιμοποιούνται για συγκεκριμένους υπηρεσιακούς σκοπούς και όχι για προσωπικούς λόγους
- Τα υπηρεσιακά δεδομένα απαγορεύεται να διαγράφονται. Η συσκευή πρέπει να χρησιμοποιείται ως backup και όχι ως το πρωτεύον μέσο αποθήκευσης
- Το Μητρώο συσκευών συμπληρώνεται από τον εργαζόμενο άμεσα με τα ακριβή στοιχεία και αποστέλλεται στη Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών
- Η συσκευή φυλάσσεται σε ασφαλές σημείο και η πρόσβαση σε αυτήν γίνεται μόνο από εξουσιοδοτημένα πρόσωπα
- Η κρυπτογράφηση της συσκευής ή των αρχείων που αποθηκεύονται σε αυτήν συστήνεται (usb εξωτερικός σκληρός δίσκος)

- Τίθεται ισχυρός κωδικός πρόσβασης, ο οποίος αλλάζει ανά τακτά χρονικά διαστήματα (βλ. Οδηγίες Κωδικών Πρόσβασης)
- Απαγορεύεται η ύπαρξη μη αδειοδοτημένου (πειρατικού) λογισμικού και εφαρμογών στη συσκευή
- Πραγματοποιούνται τακτικά ενημερώσεις ασφάλειας και λειτουργικότητας του λογισμικού της εκάστοτε συσκευής
- Χρησιμοποιούνται ενημερωμένα και κατάλληλα αντιιικά προγράμματα
- Συνίσταται το αυτόματο κλείδωμα οθόνης μετά από 10 λεπτά αδράνειας

Ο Υπάλληλος λαμβάνει γνώση της παραπάνω πολιτικής μέσω του σχετικού εντύπου το οποίο καλείται να το διαβάσει και στη συνέχεια να το υπογράψει ο ίδιος και ο προϊστάμενός του. Το έντυπο αυτό βρίσκεται στο Σύστημα Υποστήριξης Υπηρεσιών Πληροφορικής – ΑΤΛΑΣ.

12.Πολιτική Αντιγράφων Ασφαλείας

12.1 Λήψη αντιγράφων ασφαλείας

Κατά τη διαδικασία λήψης των αντιγράφων ασφαλείας τηρούνται όλα τα δεδομένα που θεωρούνται κρίσιμα για τη λειτουργία του Υπουργείου, για τα δεδομένα της εργασίας των εργαζομένων και για την προστασία των υπό επεξεργασία δεδομένων.
Τα αντίγραφα ασφαλείας, ανάλογα με την περίπτωση, λαμβάνονται σε διαφορετικά μέσα αποθήκευσης. Οι σχετικές διαδικασίες για την αποθήκευση των αντιγράφων ασφαλείας έχουν ορισθεί με τρόπο και στο μέτρο που αντιστοιχεί στο είδος και στη φύση των δεδομένων, ώστε να εξασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η ασφάλεια των δεδομένων.
Ειδικότερα, χρησιμοποιούνται δύο (2) διαφορετικά μέσα αποθήκευσης:

- Tapes για διατήρηση αντιγράφων ασφαλείας των VMs
- Πολιτική αντιγράφων ασφαλείας του Microsoft Office 365 για το σύνολο των δεδομένων

Η τοποθεσία στο cloud της Microsoft πληροί τις απαιτήσεις του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR / General Data Protection Regulation), δηλαδή τα Data Center βρίσκονται εντός Ε.Ε. Η Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών οφείλει να τηρεί σε έντυπη μορφή τη σύμβαση και τους όρους με τον πάροχο.

13. Πολιτική Διαχείρισης Περιστατικών Παραβίασης

Η λειτουργία του Υπουργείου ρυθμίζεται από διαδικασίες ελέγχου για την πρόληψη παραβιάσεων δεδομένων αλλά και για τη διαχείριση και ορθή αντιμετώπισή τους. Οι διαδικασίες και οι επιμέρους οδηγίες για τον εντοπισμό, τη διερεύνηση και την γνωστοποίηση τυχόν παραβιάσεων περιγράφονται λεπτομερώς παρακάτω.

13.1 Προληπτικές διαδικασίες και μέτρα

- Εκπαίδευση – ευαισθητοποίηση εργαζομένων για θέματα ασφάλειας και προστασίας δεδομένων (GDPR, κλπ).
- Εκπαίδευση εργαζομένων σχετικά με τα περιστατικά παραβίασης
- Εφαρμογή Πολιτικών Ασφαλείας

- Επικοινωνία και συνεργασία με εξειδικευμένους συμβούλους ασφάλειας πληροφοριακών συστημάτων
- Δημιουργία ομάδας αντιμετώπισης περιστατικών παραβίασης
- Κατανομή ρόλων και αρμοδιοτήτων
- Λήψη αντιγράφων ασφαλείας
- Εφεδρικές εγκαταστάσεις λειτουργίας της πληροφοριακής υποδομής
- Εφεδρική υποδομή παροχής ρεύματος
- Κατάλληλα μέτρα φυσικής ασφάλειας (βλ. Πολιτική Φυσικής Ασφάλειας)
- Ενημερωμένα αντιικά προγράμματα
- Firewall (τείχος προστασίας)
- Χρήση IDS/IPS συστημάτων
- Χρήση VPN για ελεγχόμενη πρόσβαση στις εφαρμογές του Οργανισμού (Αλκυόνη ΙΙ κα.)
- Αναλυτές πακέτων δεδομένων[1]
- Καταγραφή log αρχείων. Εβδομαδιαίος έλεγχος για εύρεση και αποκατάσταση κενών ασφαλείας από το Τμήμα Ασφάλειας Πληροφοριών, Συστημάτων & Εφαρμογών
- Κρυπτογράφηση αρχείων, αποθηκευτικών μέσων, αντιγράφων ασφαλείας, επικοινωνιών και εφαρμογών
- Κρυπτογράφηση δεδομένων στις περιπτώσεις κατά τις οποίες απαιτείται αντιγραφή δεδομένων από απομακρυσμένο χρήστη

13.2 Αρμόδια ομάδα αντιμετώπισης περιστατικού παραβίασης

Η Ειδική ομάδα αντιμετώπισης περιστατικών παραβίασης είναι υπεύθυνη για τη διερεύνηση και αντιμετώπιση τυχόν περιστατικών παραβίασης των δεδομένων προσωπικού χαρακτήρα. Στις βασικές αρμοδιότητες της εν λόγω Ομάδας περιλαμβάνονται η καταγραφή, η ανάλυση, η αξιολόγηση των διαδικασιών και λειτουργιών, η πληροφόρηση και ενημέρωση των υπαλλήλων του Υπουργείου, ο σχεδιασμός και η βελτίωση αντιμετώπισης έκτακτων περιστατικών παραβίασης.

13.3 Καταγραφή παραβίασης - Μητρώο καταγραφής περιστατικών

Στο Υπουργείο τηρείται μητρώο καταγραφής περιστατικών παραβίασης για όλα τα περιστατικά που εντοπίζονται. Το μητρώο συμπληρώνεται για οποιαδήποτε παραβίαση δεδομένων, ανεξάρτητα από τη σοβαρότητα ή την έκβαση αυτής. Οι συμπληρωμένες φόρμες καταχωρούνται στον φάκελο περιστατικών παραβίασης (ηλεκτρονικά ή/και σε έντυπη μορφή) και εξετάζονται σε σχέση με τα υπάρχοντα αρχεία, ώστε διαπιστωθούν τυχόν επανεμφανίσεις. Κατ' ελάχιστον, πρέπει να καταγράφονται τα ακόλουθα:

- Κατάσταση εξέλιξης περιστατικού παραβίασης (έναρξη/σε εξέλιξη, ολοκληρωμένο)
- Ημερομηνία και ώρα έναρξης/ εκδήλωσης του περιστατικού
- Ημερομηνία και ώρα που έγινε αντιληπτό το περιστατικό από τον υπάλληλο

[1] Ο αναλυτής πακέτων είναι εφαρμογή Η/Υ που χρησιμοποιείται για την παρακολούθηση και την καταγραφή της κίνησης δικτύου. Αναλύει την κυκλοφορία δικτύου και δημιουργεί μια εξατομικευμένη αναφορά, ώστε να βοηθηθούν οι οργανισμοί στη διαχείριση των δικτύων τους. Ο αναλυτής πακέτων είναι γνωστός ως ανιχνευτής, αναλυτής δικτύου ή αναλυτής πρωτοκόλλων.

- Σύντομη περιγραφή του περιστατικού
- Άλλα σχετιζόμενα περιστατικά, εφόσον υπάρχουν
- Σημείο στο οποίο εκδηλώθηκε το περιστατικό (σύστημα, υπηρεσία, εφαρμογή, τύπος δεδομένων)
- Συλλεχθέντα στοιχεία για τη διερεύνηση του περιστατικού (αρχεία καταγραφής, στοιχεία παραβίασης, μαρτυρίες κ.α.)
- Σχόλια και απόψεις των εμπλεκομένων σχετικά με το περιστατικό
- Μέτρα που πρέπει να ληφθούν για περιορισμό η εξάλειψη του κινδύνου
- Έκθεση αξιολόγησης και αντιμετώπισης περιστατικού
- Γνωστοποίηση περιστατικού, όπου απαιτείται, στις αρμόδιες Αρχές (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα - ΑΠΔΠΧ, Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - Εθνικό CERT (Ε.Υ.Π), Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΕΛ.ΑΣ.), κλπ). Επίσης, εφόσον προβλέπεται, πραγματοποιείται γνωστοποίηση του συμβάντος στο/ α υποκείμενο/ α των δεδομένων.

Πρόσβαση στο μητρώο καταγραφής περιστατικών έχει η Ομάδα Αντιμετώπισης Περιστατικών Παραβίασης.

13.4 Γνωστοποιήσεις

Οι παραβιάσεις δεδομένων προσωπικού χαρακτήρα γνωστοποιούνται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ.) υπό τους όρους του Γενικού Κανονισμού για την προστασία δεδομένων (ΓΚΠΔ.)

- Γνωστοποίηση στην ΑΠΔΠΧ
- Γνωστοποίηση στο υποκείμενο των δεδομένων (φυσικά πρόσωπα)
- Γνωστοποίηση στην Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - Εθνικό CERT (Ε.Υ.Π)
- Γνωστοποίηση στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΕΛ.ΑΣ.).

14.Πολιτική Ασφάλειας Κινητών Συσκευών – Φορητών Μέσων

14.1 Ειδικές οδηγίες και κανόνες

- Το Αρμόδιο Τμήμα είναι αρμόδιο για την παράδοση – παραλαβή κινητού εξοπλισμού, καθώς και για τον έλεγχο της ακεραιότητας αυτών κατά την επιστροφή τους στον φορέα.

- Η τακτική δημιουργία αντιγράφων ασφαλείας των αρχείων, των φακέλων και των ρυθμίσεων από τους χρήστες είναι σημαντική ώστε να είναι δυνατή η ανάκτηση δεδομένων σε περίπτωση κλοπής της κινητής συσκευής ή σε περίπτωση καταστροφής του σκληρού δίσκου.

- Η συχνότητα δημιουργίας αντιγράφων ασφαλείας των αρχείων εξαρτάται από τον αριθμό των αρχείων και τη συχνότητα με την οποία τα δημιουργούν οι χρήστες. Αν δημιουργούνται αρχεία κάθε ημέρα, συνίσταται να δημιουργούνται τα αντίγραφα ασφαλείας τους εβδομαδιαία ή και σε καθημερινή βάση. Τα αντίγραφα ασφαλείας των δεδομένων δημιουργούνται στο cloud (OneDrive). Συνίσταται ο προγραμματισμός τακτικών, αυτόματων αντιγράφων ασφαλείας, όσο εργάζεται ο χρήστης στο φορητό του υπολογιστή. Για

περισσότερες πληροφορίες, ανατρέξτε στην πολιτική αντιγράφων ασφαλείας ΠΟΛ-12 Πολιτική Αντιγράφων Ασφαλείας.

14.2 Ειδικές προϋποθέσεις ασφάλειας

Από τους ευκολότερους και πιο οικονομικούς τρόπους ασφάλισης του φορητού υπολογιστή είναι ένα καλώδιο ασφαλείας, με ή χωρίς συναγερμό, που συνδέει το φορητό υπολογιστή με ένα σταθερό αντικείμενο. Οι περισσότεροι φορητοί υπολογιστές έχουν θύρες ασφαλείας στο πλάι ή στο πίσω μέρος του περιβλήματός τους.

Μην αφήνετε ποτέ το φορητό υπολογιστή σε ένα ξεκλείδωτο δωμάτιο, ακόμα και αν το δωμάτιο θεωρείται ασφαλές.

14.3 Έλεγχος εισόδου εξόδου κινητών συσκευών

Σε περίπτωση εξόδου κινητής συσκευής από τον φορέα ενημερώνεται το Αρμόδιο Τμήμα από τον κάτοχό της κινητής συσκευής ώστε να δοθεί η γραπτή έγκριση του εν λόγω τμήματος ή του αρμόδιου προϊσταμένου.

Η κινητή και ακίνητη περιουσία του Υπουργείου έχει απογραφεί για τον καλύτερο έλεγχο.

Ο συγκεκριμένος εξοπλισμός παραδίδεται και συντάσσεται το έντυπο *Πρωτόκολλο Παραλαβής – Παράδοσης Κινητού Εξοπλισμού*, προκειμένου τα απομακρυσμένα περιουσιακά στοιχεία να τηρούνται υπό τον έλεγχο του φορέα.

14.4 Καταστροφή κινητών συσκευών

Κατόπιν απόσυρσης των κινητών συσκευών και των φορητών αποθηκευτικών μέσων αυτά καταστρέφονται (πλήρης φυσική καταστροφή – απομαγνητισμός) και διαγράφονται τα δεδομένα τους με ιδιαίτερη έμφαση στα δεδομένα προσωπικού χαρακτήρα.

15.Πολιτική Χρήσης Αποθηκευτικών Μέσων και Εγγράφων

15.1 Ειδικές οδηγίες και κανόνες

Η δυνατότητα χρήσης ή εγγραφής σε αφαιρούμενα αποθηκευτικά μέσα (CD εγγραφής, usb memory sticks, αφαιρούμενοι σκληροί δίσκοι κλπ.) είναι απενεργοποιημένη σε ηλεκτρονικούς υπολογιστές (pc και laptop).

Μόνον σε εξαιρετικά σπάνιες περιπτώσεις μπορεί να επιτραπεί η χρήση αφαιρούμενων αποθηκευτικών μέσων για την αποθήκευση δεδομένων υπηρεσιακού χαρακτήρα

Η ενεργοποίηση της δυνατότητας χρήσης τέτοιων συσκευών, πραγματοποιείται μόνο κατόπιν αίτησης του χρήστη για την αιτιολογημένη εξυπηρέτηση των υπηρεσιακών αναγκών (π.χ. δημιουργία αντιγράφων ασφάλειας ή μεταφορά εγγράφων σε κάποιο εξωτερικό συνεργάτη ή υπηρεσία) και για συγκεκριμένο χρονικό διάστημα, αφού λάβει πρώτα έγκριση από δύο ανωτέρους του, Προϊσταμένους και τελική ενυπόγραφη έγκριση από το αρμόδιο τμήμα της Γ.Δ. Πληροφορικής και Επικοινωνιών.

- Η φόρτιση συσκευών (κινητά, φορητά mp3/mp4 κτλ.), δεν επηρεάζεται από την συγκεκριμένη πολιτική. Η λειτουργικότητα autorun παραμένει απενεργοποιημένη σε όλους τους σταθμούς εργασίας

- Το αίτημα υποβάλλεται τουλάχιστον μία (1) ημέρα πριν την επιθυμητή ημερομηνία χρήσης προκειμένου να πραγματοποιηθούν έγκαιρα οι απαραίτητες ενέργειες
- Μεταφέρονται από τον υπάλληλο μόνο τα αρχεία για τα οποία έχει υποβληθεί η αίτηση και έχει εγκριθεί από τον προϊστάμενο του υπαλλήλου. Σε περίπτωση μεταφοράς μη-εγκεκριμένου αρχείου, αυτό συνιστά παραβίαση της παρούσας πολιτικής και επιφέρει κυρώσεις
- Απαγορεύεται η χρήση αφαιρούμενων μέσων αποθήκευσης σε υλικό που δεν θεωρείται ασφαλές
- Μετά το πέρας της μεταφοράς των απαραίτητων αρχείων, ενημερώνεται το Αρμόδιο Τμήμα από τον υπάλληλο μέσω του Συστήματος Υποστήριξης Υπηρεσιών Πληροφορικής «ΑΤΛΑΣ», προκειμένου να ενεργοποιηθεί εκ νέου ο περιορισμός χρήσης αφαιρούμενων μέσων αποθήκευσης
- Όλα τα αρχεία (και αντίγραφα αυτών) που περιέχουν υπηρεσιακά δεδομένα του Υπουργείου καταστρέφονται, αν και εφ' όσον αυτά δεν είναι αναγκαία, μετά το πέρας των ως άνω αναφερόμενων εργασιών
- Οι αφαιρούμενες συσκευές αποθήκευσης που έχουν χρησιμοποιηθεί για την αποθήκευση προσωπικών δεδομένων και που, είτε είναι ελαττωματικές, είτε δεν είναι πλέον απαραίτητες, επιστρέφονται στο Αρμόδιο Τμήμα
- Η καταστροφή των αφαιρούμενων συσκευών στις οποίες έχουν αποθηκευτεί υπηρεσιακά δεδομένα πραγματοποιείται βάσει των προτύπων ασφαλούς καταστροφής αποθηκευτικών μέσων
- Αποφεύγεται, όπου είναι εφικτό, η εκτύπωση διαβαθμισμένων υπηρεσιακών δεδομένων από μη εξουσιοδοτημένους χρήστες
- Αφαιρούνται άμεσα οι εκτυπώσεις ή φωτοαντίγραφα από τους εκτυπωτές και τα φωτοτυπικά μηχανήματα του Υπουργείου
- Αποθηκευτικά μέσα και έγγραφα που περιέχουν δεδομένα υπηρεσιακού χαρακτήρα, όταν δεν είναι σε χρήση, αποθηκεύονται σε κλειδωμένα συρτάρια ή φωριαμούς ή ειδικά σχεδιασμένους για το σκοπό αυτό χώρους, ώστε να είναι προσβάσιμα μόνο σε εξουσιοδοτημένους εργαζόμενους
- Δυνατότητα πρόσβασης σε αποθηκευτικά μέσα και έγγραφα που περιέχουν δεδομένα απόρρητου χαρακτήρα έχουν μόνο εξουσιοδοτημένα άτομα, βάσει καταγεγραμμένων διαδικασιών

15.2 Διακίνηση αποθηκευτικών μέσων και εγγράφων

Η μεταφορά των αποθηκευτικών μέσων και των εγγράφων περιορίζεται στο ελάχιστο δυνατό.

Για τη μεταφορά αποθηκευτικών μέσων ή εγγράφων που περιέχουν δεδομένα υπηρεσιακού χαρακτήρα, χρησιμοποιούνται ασφαλείς συσκευασίες με επισημασμένο το όνομα του παραλήπτη. Σε περίπτωση μεταφοράς δεδομένων σε αποθηκευτικά μέσα, τα δεδομένα κρυπτογραφούνται, ενώ έχουν πρόσβαση στα κλειδιά κρυπτογράφησης μόνο εξουσιοδοτημένοι χρήστες.

Τα πακέτα μεταφοράς αποθηκευτικών μέσων ή εγγράφων πρωτοκολλούνται και αποστέλλονται με ειδικά επιλεγμένες εταιρίες ταχυμεταφορών (λίστα συμβεβλημένων εταιρειών ταχυδρομείου).

Οι εταιρείες ταχυμεταφορών επιλέγονται βάσει καταγεγραμμένων διαδικασιών και έχουν συμβατικά δεσμευτεί, ώστε να διασφαλίζουν την αξιοπιστία και την εμπιστευτικότητα των παρεχόμενων υπηρεσιών.

Οποιοδήποτε αποθηκευτικό μέσο ή έγγραφο αποστέλλεται με δημόσιο ταχυδρομείο ή τρίτη εταιρεία, συσκευάζεται κατάλληλα ώστε να προστατεύεται όσο το δυνατόν καλύτερα από φυσική καταστροφή ή αλλοίωση.

15.3 Καταστροφή αποθηκευτικού μέσου ή εγγράφου

Τα στοιχεία που δεν απαιτείται πλέον η διατήρησή τους ή εμπεριέχονται σε επαναχρησιμοποιούμενα αποθηκευτικά μέσα που πρόκειται να αλλάξουν χρήση, διαγράφονται με ασφαλή τρόπο.

Επίσης, στην περίπτωση που τα αποθηκευτικά μέσα προορίζονται για απόσυρση, καταστρέφονται, αφού πρώτα διαγραφούν με ασφαλή τρόπο όλα τα αποθηκευμένα δεδομένα (secure wipe).

16.Πολιτική Ασφάλειας Antivirus

Όλα τα μηχανήματα που εντάσσονται στην εφαρμογή της παρούσας, έχουν εγκατεστημένο πρόγραμμα antivirus FortiClient, το οποίο είναι εγκεκριμένο από τη διοίκηση του Υπουργείου. Το πρόγραμμα antivirus σκανάρει το σύστημα για ιούς ανά τακτά χρονικά διαστήματα, ενώ πραγματοποιείται και έλεγχος για νέα αρχεία, εισερχόμενα ή εξερχόμενα email, σε πραγματικό χρόνο.

- Το antivirus, αλλά και η λίστα ιών ενημερώνονται τακτικά για προσθήκες και βελτιώσεις με αυτοματοποιημένο τρόπο.
- Τα μηχανήματα που έχουν προσβληθεί από ιούς αποσυνδέονται από το δίκτυο του Υπουργείου, μέχρι να επιβεβαιωθεί ότι δεν είναι μολυσμένα
- Το τμήμα Ασφάλειας ρυθμίζει τις χρονικές παραμέτρους για το αυτοματοποιημένο scan για ιούς στον server
- Στις υπηρεσιακές συσκευές χρησιμοποιείται πάντα το εγκεκριμένο από τη διοίκηση του Υπουργείου antivirus πρόγραμμα, ενώ πραγματοποιούνται τακτικά οι απαραίτητες ενημερώσεις

17. Πολιτική Κρυπτογράφησης

17.1 Ειδικές οδηγίες και κανόνες

Η κρυπτογράφηση αποτελεί πρόσφορο τεχνικό μέτρο αντιμετώπισης συμβάντος απώλειας ή κλοπής δεδομένων, όπως μνημονεύεται και στο άρθρο 32 του ΓΚΠΔ.

Ένα υποσύνολο αρχείων ή φακέλων ή ένας ολόκληρος δίσκος μπορούν να κρυπτογραφηθούν με σκοπό την προστασία των δεδομένων, του λειτουργικού συστήματος και των εγκαταστημένων προγραμμάτων.

Τα υπηρεσιακά δεδομένα αποθηκεύονται, σε εξαιρετικές περιπτώσεις, σε φορητές συσκευές αυστηρώς κρυπτογραφημένα. Η κρυπτογράφηση των αποθηκευτικών μέσων δεν απενεργοποιείται.

Τα συνημμένα αρχεία που διακινούνται μέσω αλληλογραφίας και περιέχουν ευαίσθητα προσωπικά δεδομένα αλλά και κρίσιμες υπηρεσιακές πληροφορίες, κρυπτογραφούνται μέσω λογισμικού ασύμμετρης κρυπτογράφησης.

Οι επικοινωνίες μεταξύ των φορητών συσκευών και των εσωτερικών πληροφοριακών συστημάτων του Υπουργείου είναι κρυπτογραφημένες. Για την επικοινωνία με τα εσωτερικά πληροφοριακά συστήματα χρησιμοποιούνται μόνο συνδέσεις που επιτρέπονται ρητά από ένα τείχος προστασίας.

Κατά την υλοποίηση κρυπτογράφησης λαμβάνονται υπόψιν τα εξής:

1. Ο αλγόριθμος. Θα πρέπει να είναι κατάλληλος για τη χρήση που προορίζεται και αξιολογείται τακτικά
2. Το μέγεθος του κλειδιού. Θα πρέπει να είναι αρκετά μεγάλο ώστε να προστατεύει από επιθέσεις και η καταλληλόλητά του αξιολογείται τακτικά
3. Το λογισμικό. Θα πρέπει να ανταποκρίνεται στα τρέχοντα πρότυπα, όπως FIPS 140-2 και FIPS 197
4. Την ασφάλεια του κλειδιού. Προβλέπεται διαδικασία για τη δημιουργία νέων κλειδιών, τα οποία τηρούνται σε ασφαλές σημείο

18.Πολιτική Τήρησης Δεδομένων

Οι γενικοί κανόνες τήρησης δεδομένων προσαρμόζονται και αξιολογούνται, σύμφωνα με την κείμενη και ισχύουσα νομοθεσία, επομένως ο χρόνος τήρησης εξαρτάται πρωτίστως από την ισχύουσα νομοθεσία και δευτερευόντως από την υπηρεσιακή αναγκαιότητα. Ενδεικτικά η ισχύουσα νομοθεσία ανά κατηγορία δεδομένων που ενδέχεται να υπάγεται ο Οργανισμός.

18.1 Χρόνος διατήρησης

ΕΠΕΞΕΡΓΑΣΙΑ-ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΧΡΟΝΟΣ ΔΙΑΤΗΡΗΣΗΣ
1. Φάκελος εργαζομένων	α) 5+1 έτη από τη λήξη του ημερολογιακού έτους της αποχώρησης του εργαζομένου, εξαιρουμένης της περίπτωσης έγερσης αξίωσης εντός της πενταετίας είτε από τον εργαζόμενο είτε από τον φορολογικό έλεγχο οπότε και ο χρόνος παρατείνεται στα 20 έτη (γενική παραγραφή). β) Ειδικότερα, η ατομική σύμβαση και ο πίνακας προσωπικού που αφορά τις βάρδιες, ωράριο, υπερεργασία διατηρείται για 20 έτη για την περίπτωση ελέγχου από τον ασφαλιστικό φορέα (Ν.4387/2016, άρ.95). Γενικός κανόνας: Οτιδήποτε μπορεί να δικαιολογήσει την παράταση του ως άνω χρονικού διαστήματος αιτιολογείται ειδικώς. Ο χρόνος δύναται κατά περίπτωση να ανέλθει ως την 20ετία από την αποχώρηση του εργαζόμενου.
2. Φορολογικά στοιχεία-παραστατικά	α) 5+1 έτη από την λήξη του ημερολογιακού έτους έκδοσης του σχετικού παραστατικού με δυνατότητα περαιτέρω διατήρησης σε περίπτωση ή

	εκκρεμούς διένεξης ή έγερσης δικαστικής αξίωσης ή για φορολογικούς/ασφαλιστικούς ελέγχους. β) Ο ως άνω χρόνος παρατείνεται έως τα 10 έτη, σε περίπτωση ελέγχου και δύναται να ανέλθει έως τα 20 έτη σε περίπτωση φορολογικού ελέγχου.
3. Αρχείο καταγραφής κλειστού κυκλώματος	α) Τα δεδομένα τηρούνται για το μικρότερο δυνατό χρονικό διάστημα. Για την εκπλήρωση του σκοπού επεξεργασίας που αφορά στην ασφάλεια και προστασία τόσο των προσώπων που βρίσκονται στις εγκαταστάσεις του Υπουργείου (λ.χ. εργαζόμενοι, επισκέπτες, κ.λπ.), όσο και του εν γένει εξοπλισμού λ.χ. κτηριακού, ηλεκτρονικού, κ.λπ.), τα δεδομένα δεν επιτρέπεται να τηρούνται για διάστημα μεγαλύτερο των δεκαπέντε (15) ημερών, πλην εξαιρέσεων. Εν προκειμένω λόγω του αντικειμένου και της φύσης των δραστηριοτήτων του Υπουργείου, το υλικό δύναται να διατηρηθεί έως και 45 ημέρες (βλ. και άρθρο 16 Οδηγίας 1/2011 ΑΠΔΠΧ). Μετά την παρέλευση του προβλεπόμενου χρονικού διαστήματος από τον χρόνο εισόδου του Υποκειμένου στις εγκαταστάσεις του Υπουργείου, ο σχετικός φάκελος, με το σύνολο των στοιχείων του, διαγράφεται β) Ο χρόνος τήρησης παρατείνεται, εφόσον λάβει χώρα κάποιο συμβάν και το υλικό μπορεί να χρησιμοποιηθεί ως αποδεικτικό στοιχείο (βλ. άρ. 8 της Οδηγίας 1/2011 της ΑΠΔΠΧ, για αναλυτικότερη περιγραφή, καθώς και το αντίστοιχο άρθρο του Ειδικού Μέρους της Οδηγίας, ανάλογα με την κατηγορία του Υπευθύνου Επεξεργασίας). Σε περίπτωση συμβάντος (λ.χ. κλοπή, ληστεία, ξυλοδαρμός σε βάρος του προσώπου ή των αγαθών του Υπεύθυνου Επεξεργασίας), επιτρέπεται να τηρούνται οι εικόνες στις οποίες έχει καταγραφεί το συγκεκριμένο συμβάν, σε χωριστό αρχείο για χρονικό διάστημα τριάντα (30) ημερών και επιπλέον, εάν το συμβάν αφορά τρίτο πρόσωπο, ο Υπεύθυνος Επεξεργασίας τηρεί τις εικόνες για χρονικό διάστημα τριών (3) μηνών.
4. Τήρηση αρχείου συμβάσεων	α) ως προς τα δεδομένα που συλλέγονται στο πλαίσιο σύναψης και εκτέλεσης της σύμβασης, διατήρηση αυτών για χρονικό διάστημα ανάλογο της διάρκειας της σύμβασης. β) σε περίπτωση λήξης της σύμβασης, για χρονικό διάστημα είκοσι (20) ετών από τη λήξη της (γενική παραγραφή), γ) σε περίπτωση μη σύναψης της σύμβασης, διατήρηση των δεδομένων στο αρχείο για διάστημα πέντε (5) ετών. Οι ως άνω χρόνοι δύνανται να παραταθούν, εάν εκκρεμεί δικαστική διένεξη πέραν των ως άνω χρόνων επεξεργασίας και μέχρι την περαίωσή της με αμετάκλητη δικαστική απόφαση.

18.2 Διαγραφή καταστροφή

Τα προσωπικά δεδομένα καταστρέφονται με ασφαλή τρόπο, ώστε να αποκλειστεί η περαιτέρω μη νόμιμη και αθέμιτη επεξεργασία τους.

α. Φυσικό αρχείο: Εφόσον παρέλθει ο χρόνος διατήρησης ή σε περίπτωση αιτήματος, το οποίο κρίνεται ότι μπορεί να ικανοποιηθεί, διαγράφονται τα αντίστοιχα προσωπικά δεδομένα. Για την οριστική διαγραφή προσωπικών δεδομένων που υπάρχουν σε έντυπη μορφή χρησιμοποιείται καταστροφέας εγγράφων ώστε να είναι μη ανακτήσιμα, ενώ απαγορεύεται η ρίψη των εγγράφων σε κάδο σκουπιδιών.

β. Ηλεκτρονικό αρχείο: Εφόσον παρέλθει ο χρόνος διατήρησης ή σε περίπτωση αιτήματος, το οποίο κρίνεται ότι μπορεί να ικανοποιηθεί, διαγράφονται τα αντίστοιχα προσωπικά δεδομένα, από όλες τις τοποθεσίες που αυτά είναι αποθηκευμένα.

19. Πολιτική χρήσης υπηρεσιών Νέφους (Cloud)

Η παρούσα πολιτική περιγράφει τις αρχές που ακολουθούνται κατά τη χρήση υπηρεσιών οι οποίες παρέχονται μέσω υποδομών Cloud προκειμένου να διασφαλίζεται η εμπιστευτικότητα, διαθεσιμότητα και ακεραιότητα των πληροφοριών που επεξεργάζεται το Υπουργείο. Ως υπηρεσίες Cloud ορίζονται οι υπηρεσίες οι οποίες διατίθενται σε χρήστες στο διαδίκτυο μέσω των υποδομών του παρόχου των υπηρεσιών. Διακρίνονται οι ακόλουθες περιπτώσεις υπηρεσιών Cloud:

Software as a Service (SaaS): Παρέχεται η δυνατότητα χρήσεως εφαρμογών οι οποίες φιλοξενούνται σε υποδομές νέφους του παρόχου υπηρεσιών. Οι εφαρμογές είναι προσβάσιμες από διάφορους τύπους συσκευών μέσω browser. Οι χρήστες της συγκεκριμένης υπηρεσίας δεν διαχειρίζονται ούτε ελέγχουν τις υποστηρικτικές υποδομές συμπεριλαμβανομένων των servers, του δικτύου, των λειτουργικών συστημάτων, των αποθηκευτικών μέσων ή ακόμα και των δυνατοτήτων των εφαρμογών παρά μόνο συγκεκριμένων χαρακτηριστικών παραμετροποιήσεως.

Platform as a Service (PaaS): Παρέχεται η δυνατότητα εγκατάστασης σε υποδομές Cloud εφαρμογών. Οι χρήστες της συγκεκριμένης υπηρεσίας δεν διαχειρίζονται ούτε ελέγχουν τις υποστηρικτικές υποδομές συμπεριλαμβανομένων των servers, του δικτύου, των λειτουργικών συστημάτων, των αποθηκευτικών μέσων. Έχουν τη δυνατότητα ελέγχου των εφαρμογών που έχουν εγκαταστήσει στις Cloud υποδομές.

Infrastructure as a Service (IaaS): Παρέχονται πληροφοριακές υποδομές όπως επεξεργαστές, αποθηκευτικά μέσα, δίκτυα, στα οποία ο χρήστης μπορεί να εγκαταστήσει προγράμματα λογισμικού, όπως λειτουργικά συστήματα και εφαρμογές. Οι χρήστες των υπηρεσιών δεν έχουν τη δυνατότητα διαχειρίσεως των υποστηρικτικών φυσικών υποδομών, ωστόσο μπορούν να ελέγχουν και να διαχειρίζονται το λειτουργικό σύστημα, το χώρο αποθηκεύσεως και τις εφαρμογές. Επιπρόσθετα, ενδέχεται να έχουν περιορισμένες δυνατότητες διαχειρίσεως σε δικτυακό εξοπλισμό (π.χ. firewalls).

Για την κάλυψη των επιχειρησιακών αναγκών του ΥΜΑ, αξιολογούνται, εκτός των υλοποιήσεων που βασίζονται σε ιδιόκτητες υποδομές, λύσεις που στηρίζονται στη χρήση υπηρεσιών Cloud. Οι υπηρεσίες Cloud προσφέρουν μία σειρά πλεονεκτημάτων όπως:

- Επεκτασιμότητα υποδομών

- Ευκολία αναπτύξεως συστημάτων
- Αυξημένα επίπεδα διαθεσιμότητας
- Μικρότερο διαχειριστικό κόστος
- Προσβασιμότητα

Οι υπηρεσίες Cloud προσφέρουν αρκετά πλεονεκτήματα, ωστόσο, η χρήση τους ενέχει κινδύνους για την Ασφάλεια Πληροφοριών εξαιτίας των ακόλουθων παραγόντων:

- Αδυναμία ελέγχου των εφαρμοζόμενων μέτρων Ασφαλείας Πληροφοριών
- Πρόσβαση από τρίτους σε πληροφορίες του ΥΜΑ
- Ελλιπή αρχιτεκτονική των υποστηρικτικών πληροφοριακών συστημάτων
- Μη ικανοποίηση κανονιστικών και νομικών απαιτήσεων

Οι αιτήσεις των Διευθύνσεων του ΥΜΑ για χρήση υπηρεσιών Cloud εξετάζονται ανά περίπτωση από τον Υπεύθυνο Ασφάλειας Πληροφοριών. Ειδικότερα, αξιολογούνται οι κίνδυνοι που είναι δυνατόν να οδηγήσουν σε διακοπή επιχειρησιακών δραστηριοτήτων, διαρροή δεδομένων ή παραβίαση της Ασφάλειας Πληροφοριών του ΥΜΑ. Στη συνέχεια, προσδιορίζονται τα μέτρα ασφάλειας που εφαρμόζονται για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφορίων που διαχειρίζεται το ΥΜΑ κατά τις ακόλουθες φάσεις:

- Δημιουργία των πληροφοριών
- Επεξεργασία
- Αποθήκευση
- Μεταφορά
- Καταστροφή

Η χρήση υπηρεσιών Cloud ενέχει υψηλό κίνδυνο διαρροής ή μη εξουσιοδοτημένης προσβάσεως σε δεδομένα του ΥΜΑ. Κακόβουλες ενέργειες είναι δυνατόν να υλοποιηθούν τόσο κατά τη μεταφορά των δεδομένων μεταξύ του ΥΜΑ και των υποδομών Cloud όσο κατά τη φάση της επεξεργασίας και της αποθήκευσής τους. Η προστασία τους εξαρτάται από την ισχύ των μέτρων που εφαρμόζει ο πάροχος των υπηρεσιών, αλλά και το ίδιο το ΥΜΑ. Το πλήθος και το είδος των μέτρων καθορίζονται από:

- Το επίπεδο διαβαθμίσεως των πληροφοριών που μεταφέρονται στις υποδομές Cloud
- Το είδος των υπηρεσιών Cloud
- Το είδος και το επίπεδο των κινδύνων που αναγνωρίζονται κατά τη μελέτη εκτιμήσεως κινδύνων η οποία διενεργείται κατά τη φάση αξιολόγησης της υπηρεσίας Cloud

Κατά τη σύναψη συμφωνιών/συνεργασίας με παρόχους υπηρεσιών Cloud προσδιορίζονται οι ευθύνες και οι αρμοδιότητες σε σχέση με τις ενέργειες που ακολουθούνται και τα μέτρα που υλοποιούνται για την προστασία των υποδομών Cloud. Πιο συγκεκριμένα, προσδιορίζονται επακριβώς τα όρια ευθύνης για τους ακόλουθους τομείς:

- Προστασία από κακόβουλο λογισμικό
- Λήψη αντιγράφων ασφαλείας
- Αντιμετώπιση ευπαθειών
- Διαχείριση Κινδύνων
- Έλεγχοι Ασφαλείας Πληροφοριών
- Παραγωγή και διαχείριση καταγραφών

- Μηχανισμοί ελέγχου προσβάσεως και κρυπτογραφήσεως δεδομένων

Ο πάροχος των υπηρεσιών Cloud ακολουθεί καθορισμένες διαδικασίες για την υλοποίηση των μέτρων προστασίας που είναι υπό την ευθύνη του. Επιπρόσθετα, καθορίζεται ο τύπος και η συχνότητα των αναφορών οι οποίες αποστέλλονται με σκοπό την παρακολούθηση της αποτελεσματικότητας των μέτρων Ασφαλείας.

Στις συμβάσεις με παρόχους υπηρεσιών Cloud προσδιορίζεται το επίπεδο των παρεχόμενων υπηρεσιών καθώς και οι μέθοδοι παρακολούθησής του. Ο πάροχος των υπηρεσιών Cloud θα πρέπει να προσφέρει τα εργαλεία που απαιτούνται ώστε το ΥΜΑ να μπορεί να παρακολουθεί σε συνεχή βάση τη χρονική εξέλιξη του επιπέδου των παρεχόμενων υπηρεσιών. Καθορίζονται επίσης, τα είδη των αναφορών και η συχνότητα αποστολής τους ώστε το Υπουργείο να μπορεί να ελέγχει παραμέτρους όπως:

- Αποκλίσεις από το καθορισμένο επίπεδο παροχής υπηρεσιών
- Χρονική διάρκεια αποκλίσεων και συχνότητα εμφανίσεώς τους
- Ενέργειες αντιμετωπίσεως αποκλίσεων

Για την αποτελεσματική αντιμετώπιση περιστατικών Ασφαλείας Πληροφοριών προσδιορίζονται τα κάτωθι:

- Τα περιστατικά ασφαλείας πληροφοριών αναφέρονται στους υπεύθυνους του ΥΜΑ και του παρόχου υπηρεσιών Cloud
- Τα στοιχεία επικοινωνίας των υπευθύνων (τηλέφωνο, email)
- Οι ενέργειες που ακολουθούνται κατά την αναφορά περιστατικών Ασφαλείας Πληροφοριών
- Τα στοιχεία που γνωστοποιούνται κατά την ενημέρωση ύπαρξης περιστατικού Ασφαλείας Πληροφοριών

Τα ανωτέρω στοιχεία καταγράφονται στις συμβάσεις που συνάπτει το ΥΜΑ με παρόχους υπηρεσιών Cloud. Επιπρόσθετα, προσδιορίζεται η υποχρέωση του παρόχου των υπηρεσιών να ενημερώνει άμεσα το ΥΜΑ στην περίπτωση εντοπισμού περιστατικού Ασφαλείας, ώστε να είναι δυνατή η έγκαιρη και αποτελεσματική αντιμετώπισή του.

Προκειμένου το ΥΜΑ να διασφαλίζει τη συνέχεια των επιχειρησιακών του λειτουργιών που προσφέρονται μέσω υποδομών Cloud, λαμβάνει τα απαραίτητα μέτρα προκειμένου να είναι εφικτή και αποτελεσματική η μεταφορά των υπηρεσιών σε άλλους παρόχους ή σε ιδιόκτητες υποδομές. Για το λόγο αυτό:

- Αναπτύσσει και υλοποιεί πλάνα εξόδου τα οποία είναι ολοκληρωμένα, τεκμηριωμένα και δοκιμασμένα, όπου αυτό είναι εφικτό.

- Προσδιορίζει εναλλακτικούς παρόχους υπηρεσιών και σχεδιάζει πλάνα μεταφοράς υπηρεσιών

- Διασφαλίζει ότι οι συμβάσεις με παρόχους υπηρεσιών Cloud περιλαμβάνουν όρους που σχετίζονται με:

- Την υποχρέωση των παρόχων να υποστηρίξουν το ΥΜΑ κατά τη φάση της μετάβασης ώστε να ελαχιστοποιηθεί η πιθανότητα μη διαθεσιμότητας των επιχειρησιακών του λειτουργιών

- Την υποχρέωση των παρόχων να παραδώσουν στο ΥΜΑ το σύνολο των δεδομένων που τηρούνται στις υποδομές του και να τα διαγράψει ασφαλώς από αυτές.

ΠΑΡΑΡΤΗΜΑ Ι: ΔΕΛΤΙΟ ΧΡΕΩΣΗΣ ΨΗΦΙΑΚΟΥ ΚΛΕΙΔΙΟΥ

Άγιος Ιωάννης Ρέντης, _____._____ . 20__

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΜΕΤΑΝΑΣΤΕΥΣΗΣ ΚΑΙ ΑΣΥΛΟΥ

Γ.Δ. ΠΛΗΡΟΦΟΡΙΚΗΣ & ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ, ΣΥΣΤΗΜΑΤΩΝ & ΕΦΑΡΜΟΓΩΝ

Δελτίο χρέωσης Ψηφιακού Κλειδιού και Κανόνες Απομακρυσμένης Πρόσβασης στις Υποδομές της Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνών του Υπουργείου Μετανάστευσης και Ασύλου για υπαλλήλους Υπουργείου.

Με το παρόν παρέχεται στ_____,
υπάλληλο Διεύθυνσης _____,
του Τμήματος _____,
αριθμό τηλεφώνου_____, email _____,

σύμβαση εργασίας_____, Domain User Name_____
_____ και όνομα υπολογιστή _____, το δικαίωμα ασφαλής απομακρυσμένης πρόσβασης μέσω της εφαρμογής *FortiClient VPN* στα Πληροφοριακά Συστήματα που φιλοξενούνται στο κτίριο Κεράνη, Θηβών 196-198, Άγιος Ιωάννης Ρέντης, στο Data Center της Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών στον 6ο όροφο του Υπουργείου Μετανάστευσης και Ασύλου.

Επισημαίνεται ότι η σύνδεση απομακρυσμένης επιφάνειας εργασίας επιτρέπεται μόνο στον υπηρεσιακό υπολογιστή του υπαλλήλου στον οποίο έχει εκχωρηθεί το δικαίωμα πρόσβασης εξ αποστάσεως μέσω την εφαρμογής των Windows Remote Desktop.

Στον VPN Server διατηρείται το ηλεκτρονικό αρχείο καταγραφής ενεργειών (log file) κάθε συνεδρίας διασύνδεσης (session) για τουλάχιστον 5 έτη.

Ο χρήστης του VPN κλειδιού θα πρέπει:

1. Να περιορίζεται μόνο στην πρόσβαση / επεξεργασία των πληροφοριών που είναι απαραίτητες για την εκτέλεση των καθηκόντων που του έχουν ανατεθεί.
2. Να μην αποθηκεύει μη υπηρεσιακά αρχεία (π.χ. φωτογραφίες) στο δίκτυο και τους πόρους του Υπουργείου Μετανάστευσης και Ασύλου.
3. Να μην προβαίνει σε
   - καθ' οιονδήποτε τρόπο εκμετάλλευση πιθανών κενών ασφάλειας του ηλεκτρονικού εξοπλισμού (τηλεπικοινωνιακού, διαδικτύου κ.τ.λ.) στο οποίο του έχει επιτραπεί η πρόσβαση,
   - προσβολή ή κακή χρήση των συστημάτων, υπηρεσιών και εφαρμογών του Υπουργείου,
   - διατάραξη της ομαλής λειτουργίας των δικτύων και υπηρεσιών του Υπουργείου και

- εκτέλεση οποιουδήποτε κακόβουλου λογισμικού που δύναται να θέσει σε κίνδυνο ή να υποβαθμίσει το επίπεδο ασφάλειας των Πληροφοριακών Συστημάτων του Υπουργείου.

4. Σε περίπτωση υποψιών ή διαπίστωσης συμβάντος τρωτότητας ή διάπραξης αδικήματος που εμπλέκει τα συστήματα Πληροφορικής Τεχνολογίας, θα πρέπει να ειδοποιεί άμεσα το Τμήμα Ασφαλείας Πληροφοριών, Συστημάτων & Εφαρμογών του Υπουργείου Μετανάστευσης και Ασύλου με email στο cert@migration.gov.gr
5. Να τηρεί μυστικά τα στοιχεία των προσωπικών λογαριασμών (όνομα χρήστη, κωδικός) και να ειδοποιεί άμεσα το Τμήμα Ασφαλείας Πληροφοριών, Συστημάτων & Εφαρμογών του Υπουργείου Μετανάστευσης και Ασύλου στο email cert@migration.gov.gr για τυχόν διαρροή τους.
6. Να ανακοινώνεται εγγράφως στη Διεύθυνση Υποδομών Πληροφορικής και Επικοινωνιών του Υπουργείου Μετανάστευσης και Ασύλου η απώλεια του κωδικού πρόσβασης ώστε αυτός να απενεργοποιείται και να χορηγείται νέος.
7. Να μην κοινοποιεί σε κανέναν τρίτο με κανένα μέσο, προφορικό, γραπτό, ψηφιακό (τηλεφωνικά, μέσω email κ.τ.λ.) τους προσωπικούς κωδικούς πρόσβασής του στα προαναφερόμενα συστήματα.
8. 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).
9. Να μην παραχωρεί τους προσωπικούς κωδικούς πρόσβασης σε άλλα πρόσωπα προκειμένου να πραγματοποιήσουν υπηρεσιακό έργο επ' ονόματί του.
10. Να λαμβάνει μέριμνα ώστε να αλλάζει μια φορά το τρίμηνο περιοδικά τους κωδικούς πρόσβασής του και να αποφεύγει την χρήση του ίδιου κωδικού σε όλα τα συστήματα.
11. Να ενημερώνει άμεσα και εγγράφως, τη Διεύθυνση Υποδομών Πληροφορικής και Επικοινωνιών σχετικά με τη λήξη παροχής υποστήριξης, την αποχώρηση/μετάθεσή του από την Υπηρεσία/Φορέα που έχει εκχωρηθεί το δικαίωμα εξ αποστάσεως πρόσβασης, έτσι ώστε να γίνεται αφαίρεση των δικαιωμάτων πρόσβασης που του έχει χρεωθεί στις εφαρμογές και τα υπηρεσιακά αρχεία.
12. Να κλειδώνει με μυστικό προσωπικό κωδικό την επιφάνεια εργασίας του Η/Υ του όταν απουσιάζει από το γραφείο του.
13. Να ενημερώσει αρμοδίως την υπηρεσία του, εφόσον περιέλθει στην αντίληψή του, χρήση Η/Υ με τα προσωπικά - υπηρεσιακά περιεχόμενα υπαλλήλου ο οποίος αποχώρησε.
14. Το παρόν έντυπο διακινείται μέσω του συστήματος Υποστήριξης Υπηρεσιών Πληροφορικής «ΑΤΛΑΣ» ή του Συστήματος Ηλεκτρονικής Διακίνησης Εγγράφων ΙΡΙΔΑ, υπογράφεται από τον Προϊστάμενο Διεύθυνσης ή Τμήματος του υπηρετούντος και αποστέλλεται στην Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών του Υπουργείου Μετανάστευσης και Ασύλου.

ΥΠΟΓΡΑΦΗ ΥΠΑΛΛΗΛΟΥ	ΥΠΟΓΡΑΦΗ ΠΡΟΪΣΤΑΜΕΝΟΥ

ΠΑΡΑΡΤΗΜΑ ΙΙ: ΕΝΙΑΙΟ ΠΛΗΡΟΦΟΡΙΑΚΟ ΣΥΣΤΗΜΑ ΥΠΟΔΟΧΗΣ ΚΑΙ ΑΣΥΛΟΥ «ΑΛΚΥΟΝΗ ΙΙ»

1. Γενικές Αρχές Πολιτικής Πρόσβασης Χρηστών

Οι βασικές αρχές παροχής δικαιωμάτων πρόσβασης του Ενιαίο Πληροφοριακό Σύστημα Υποδοχής και Ασύλου είναι η αρχή των ελάχιστων δικαιωμάτων (least privilege) και της ανάγκης γνώσης (need to know basis), ήτοι ο κάθε χρήστης αποκτά πρόσβαση μόνο σε πληροφοριακούς πόρους, οι οποίοι θεωρούνται απαραίτητοι για την ομαλή διεκπεραίωση των καθημερινών εργασιών του.

Τα δικαιώματα πρόσβασης του κάθε χρήστη σε εφαρμογές και πληροφοριακά συστήματα απορρέουν από τις αρμοδιότητες, το αντικείμενο εργασίας του καθώς και από τη θέση την οποία κατέχει στα πλαίσια της οργάνωσης της Υπηρεσίας και πρέπει να ορίζονται λεπτομερώς ανάλογα με τον εργασιακό ρόλο του κάθε εργαζόμενου.

Καθορίζεται ομαδοποίηση των δικαιωμάτων πρόσβασης σε πληροφοριακά συστήματα και εφαρμογές ανά εργασιακό ρόλο (Role Based Access Control, RBAC), σύμφωνα με τις απαιτήσεις πρόσβασης κάθε ρόλου, όπως αυτές ορίζονται στο ανώτατο επίπεδο ιεραρχίας των υπηρεσιών (Υπηρεσίας Ασύλου, Υπηρεσίας Υποδοχής και Ταυτοποίησης, Αρχής Προσφυγών).

Η προστασία των δεδομένων αποτελεί σημαντικό μέτρο για την ασφάλεια του Συστήματος. Όλο το προσωπικό ενημερώνεται, κατά την τοποθέτησή του για την Πολιτική και τις Οδηγίες Ασφάλειας Πληροφοριών & Πληροφοριακών Συστημάτων της «Γενικής Δ/νσης Πληροφορικής και Επικοινωνιών/ Υ.Μ.Α.» για να εξοικειώνεται με τις αρχές της ασφάλειας πληροφοριών, υπογράφοντας σχετικό έντυπο (κοινό με το έντυπο Χορήγησης Πρόσβασης) και δεσμεύεται εγγράφως ότι αποδέχεται τους όρους της Πολιτικής και αναλαμβάνει τη δέσμευση να συμμορφώνεται με τις βασικές αρχές προστασίας δεδομένων. Επίσης, υπάρχει συνεχής ενημέρωση και παρότρυνση των χρηστών για εφαρμογή των αρχών προστασίας των δεδομένων.

Οι προϊστάμενοι των κατά τόπον υπηρεσιών πραγματοποιούν έλεγχο για την παροχή - αφαίρεση εξουσιοδοτήσεων. Ειδικότερα, για την παροχή εξουσιοδότησης σε απόρρητα για συγκεκριμένη ομάδα χρηστών (όπως οι χειριστές υποθέσεων ασύλου) πραγματοποιείται βάσει της Διαδικασίας Εξουσιοδοτήσεων που καταρτίζεται από Αυτοτελές Τμήμα Πολιτικού Σχεδιασμού Έκτακτης Ανάγκης/ΥΜΑ.

Σημειώνεται δε ότι τα δεδομένα του Ενιαίου ΠΣ Υποδοχής και Ασύλου «Αλκυόνη ΙΙ» εντάσσονται στις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα - Ευαίσθητα δεδομένα. Ευαίσθητα δεδομένα χαρακτηρίζονται μεταξύ άλλων αυτά που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές πεποιθήσεις, δεδομένα που αφορούν την υγεία, τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό του ατόμου. Σε αυτή την κατηγορία συμπεριλαμβάνονται και τα δεδομένα που είναι σχετικά με ποινικές διώξεις ή καταδίκες.

Αναλυτικές οδηγίες-κατευθύνσεις παρουσιάζονται στο κείμενο «ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ».

2. Καθορισμός δικαιωμάτων πρόσβασης

Η πρόσβαση σε υπηρεσίες και δεδομένα του Συστήματος καθορίζεται σύμφωνα με τις ανάγκες των διαφόρων Υπηρεσιών. Ο πλήρης καθορισμός αυτών ανήκει στις αρμόδιες Υπηρεσίες του Υ.Μ.Α. (ΓΔΠΕ) και πρέπει διαρκώς να ενημερώνεται.

Για κάθε χρήστη, το σύνολο των δικαιωμάτων που παραχωρούνται είναι αυτό που επιτρέπει στον χρήστη τελικά να εκτελεί όλες τις εργασίες, όπως επιβάλλονται από τις αρμοδιότητές του και τον εργασιακό ρόλο. Σε περίπτωση μεταβολής των ανωτέρω, οι υπηρεσίες υποχρεούνται να ενημερώνουν τη Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών (ΓΔΠΕ) μέσω του Συστήματος Υποστήριξης Υπηρεσιών Πληροφορικής «ΑΤΛΑΣ».

3. Διαδικασίες διαχείρισης χρηστών και προνομίων/ρόλων

Οι νέοι χρήστες δημιουργούνται βάσει των καθηκόντων και αρμοδιοτήτων τους, όπως αυτοί απορρέουν από τον εργασιακό τους ρόλο. Τα βασικά σημεία, τα οποία καλύπτονται από τη διαδικασία, είναι τα ακόλουθα:

- Οι χρήστες ενημερώνονται από τον Προϊστάμενο/Διευθυντή της οργανικής μονάδας, στην οποία υπάγονται, σχετικά με τα δικαιώματα πρόσβασης που τους έχουν δοθεί ανάλογα με το ρόλο τους στην εφαρμογή.
- Η έναρξη της διαδικασίας παροχής δικαιωμάτων πρόσβασης γίνεται κατόπιν έγκρισης του Προϊστάμενου της οργανικής μονάδας που ανήκει ο χρήστης.

Οι διαδικασίες διαχείρισης των χρηστών αποτυπώνονται στον παρακάτω πίνακα:

Πίνακας Α

Διαδικασία	**Ενέργεια**
Εισαγωγή Νέου Χρήστη	Αίτημα εισαγωγής νέου χρήστη από τον Προϊστάμενο/Διευθυντή της οργανικής μονάδας στην οποία υπάγεται ο χρήστης, στο Σύστημα Υποστήριξης Υπηρεσιών Πληροφορικής «ΑΤΛΑΣ» (εφεξής σύστημα «ΑΤΛΑΣ»)
Διαγραφή Χρήστη	Αίτημα διαγραφής χρήστη μέσω συστήματος «ΑΤΛΑΣ» από τον Προϊστάμενο/Διευθυντή της οργανικής μονάδας στην οποία υπάγεται ο χρήστης
Τροποποίηση Χρήστη	Αίτημα τροποποίησης χρήστη στο σύστημα «ΑΤΛΑΣ» από τον Προϊστάμενο/Διευθυντή της οργανικής μονάδας στην οποία υπάγεται ο χρήστης

Οι διαδικασίες Διαχείρισης Προνομίων/Ρόλων των χρηστών αποτυπώνονται στον παρακάτω πίνακα:

Πίνακας Β

Διαδικασία	**Ενέργεια**
Απόδοση Προνομίων/Ρόλων	Αίτημα απόδοσης προνομίων/ρόλων στο σύστημα «ΑΤΛΑΣ» από Προϊστάμενο/Διευθυντή της οργανικής μονάδας στην οποία υπάγεται ο χρήστης
Διαγραφή Προνομίων/Ρόλων	Αίτημα διαγραφής προνομίων στο σύστημα «ΑΤΛΑΣ» από Προϊστάμενο/Διευθυντή της οργανικής μονάδας στην οποία υπάγεται ο χρήστης

Για οποιοδήποτε αίτημα στο σύστημα «ΑΤΛΑΣ» θα πρέπει να αναφέρονται οι κάτωθι πληροφορίες:

1. Το θέμα των διαδικασιών που ζητούνται προς περαίωση, όπως αυτές περιγράφονται στους ανωτέρω πίνακες Α και Β, πχ. Θέμα: Εισαγωγή Νέου Χρήστη
2. Πλήρης περιγραφή του αιτήματος συμπεριλαμβανομένων των παρακάτω πληροφοριών:
   - Υπηρεσία: Οργανική μονάδα (Διεύθυνση, τμήμα, γραφείο, κλιμάκιο) στην οποία υπάγεται/εργάζεται ο υπάλληλος
   - Επώνυμο
   - Όνομα
   - E-mail
   - Θέση: Σε περίπτωση που κατέχει θέση ευθύνης
   - Λεκτικό υπογραφής: Σε περίπτωση που κατέχει θέση ευθύνης
   - Ρόλοι/προνόμια: Ρόλοι/προνόμια προς απόδοση/διαγραφή.

Οι ρόλοι/προνόμια ανά υπηρεσία περιγράφονται αναλυτικά σε σχετικό εγχειρίδιο που έχουν λάβει οι Υπηρεσίες από τη Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών και το οποίο επικαιροποιείται σε τακτική βάση.
Λοιπές υπηρεσίες: οργανικές μονάδες (Διεύθυνση, τμήμα, γραφείο, κλιμάκιο, δομή) που υποστηρίζει μέσω των ρόλων/προνομίων που ζητούνται προς απόδοση/διαγραφή

Όλες οι διαδικασίες που αποτυπώνονται στον Πίνακα Α (Διαδικασίες Διαχείρισης Χρηστών) και Β (Διαδικασίες Διαχείρισης Προνομίων/Ρόλων Χρηστών), εκτελούνται οριζόντια από συγκεκριμένα στελέχη της Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών (ΓΔΠΕ), εξουσιοδοτημένα με το ρόλο Διαχειριστή.

Εναλλακτικά, οι Διαδικασίες Διαχείρισης Προνομίων/Ρόλων Χρηστών που περιγράφονται στον Πίνακα Β, μπορούν να εφαρμοστούν σε επίπεδο υπηρεσίας και μόνο για τους ήδη ενεργούς χρήστες, από ειδικά εξουσιοδοτημένα στελέχη της κάθε υπηρεσίας, που έχουν τον ρόλο του τοπικού διαχειριστή σύμφωνα με το παρακάτω πίνακα:

Υπηρεσία	Τοπικός ρόλος Διαχειριστή
Υπηρεσία Ασύλου	Διαχειριστής Υπηρεσίας Ασύλου
Υπηρεσία Υποδοχής και Ταυτοποίησης	Διαχειριστής ΥΠΥΤ
Αρχή Προσφυγών	Διαχειριστής Αρχής Προσφυγών

Επισημαίνεται ότι:

- Συντηρείται κατάσταση στην οποία αναφέρονται όλοι οι χρήστες των τοπικών ρόλων διαχειριστή. Για κάθε μεταβολή της κατάστασης πρέπει να ενημερώνεται η ΓΔΠΕ.
- Τα χορηγηθέντα δικαιώματα καταγράφονται.
- Οι κωδικοί πρόσβασης των συγκεκριμένων τύπων χρηστών αλλάζονται σε τακτά χρονικά διαστήματα.
- Οι ενέργειες των συγκεκριμένων τύπων χρηστών καταγράφονται από τα εργαλεία παρακολούθησης των συστημάτων και των εφαρμογών και ελέγχονται.

4. Επανεξέταση δικαιωμάτων πρόσβασης

Οι εξουσιοδοτήσεις του προσωπικού επανεξετάζονται ανά τακτά χρονικά διαστήματα και σε κάθε περίπτωση μεταβολής της εργασίας του (ακόμα και ανάθεση διαφορετικών καθηκόντων χωρίς μετακίνηση) και μεταβάλλονται με ευθύνη του οικείου Προϊσταμένου.

Αντίστοιχα, επανεξετάζονται σε κάθε περίπτωση μεταβολής της θέσης ή της σχέσης εργασίας του (απόσπαση, μετάθεση, συνταξιοδότηση κλπ.) και ανακαλούνται.

Μετά τη λήξη της σχέσης εργασίας το προσωπικό υποχρεούται να τηρεί την εχεμύθεια και τυχόν άλλες υποχρεώσεις που απορρέουν από την ενασχόλησή του με τις πληροφορίες του Ενιαίου Π.Σ. Υποδοχής και Ασύλου.

Σε περίπτωση που απαιτηθεί χειρισμός διαβαθμισμένων πληροφοριών από ιδιώτες ή φορείς συνεργαζόμενους με οποιαδήποτε μορφή με το Υ.Μ.Α., απαιτείται εξουσιοδότηση ανάλογη του βαθμού ασφάλειας των δεδομένων στα οποία έχουν πρόσβαση. Με την εξουσιοδότηση πιστοποιείται η δυνατότητα του συγκεκριμένου προσωπικού να λαμβάνει γνώση και να χειρίζεται διαβαθμισμένες πληροφορίες, με την εχεμύθεια και μυστικότητα που επιβάλλεται από τον Κανονισμό Ασφαλείας.

5. Ευθύνη προϊσταμένων

Οι προϊστάμενοι των Υπηρεσιών του Υ.Μ.Α. πρέπει να:

- ενημερώνουν επαρκώς τους υπαλλήλους τους για το ρόλο και τις ευθύνες τους, καθώς και για τις απαιτήσεις ασφάλειας.
- πραγματοποιούν έλεγχο για περιορισμό της πρόσβασης στο Ενιαίο Πληροφοριακό Σύστημα Υποδοχής και Ασύλου (αφαίρεση προνομίων/ρόλων ή απενεργοποίηση της πρόσβασης) κατά τη χρονική στιγμή της λήξης της σχέσης εργασίας του εκάστοτε υπαλλήλου.

6. Πρόσβαση στο Σύστημα

Κάθε χρήστης είναι υπεύθυνος για την επιλογή και διαφύλαξη συνθηματικού (password) για την πρόσβαση στο λογαριασμό του, ώστε να αναγνωρίζεται μοναδικά κατά την είσοδό του στο Ενιαίο Πληροφοριακό Σύστημα Υποδοχής και Ασύλου. Τα συνθηματικά είναι αυστηρώς προσωπικά, απαγορεύεται να δίδονται σε τρίτους και δεν πρέπει να αποτυπώνονται σε χαρτί ή να φυλάσσονται σε οποιαδήποτε μορφή (ηλεκτρονική ή μη). Σε περίπτωση υποψίας ότι οι μυστικοί κωδικοί πρόσβασης έπαυσαν να είναι μυστικοί, τότε πρέπει να τροποποιούνται άμεσα.

- Το Ενιαίο Πληροφοριακό Σύστημα Υποδοχής και Ασύλου εγκαθίσταται στους Η/Υ με κλειδί που φέρει μοναδικό κωδικοποιημένο όνομα.
- Πριν την επιλογή κωδικού πρόσβασης/αναγνώρισης (password), οι χρήστες πρέπει να συμβουλευτούν το κεφ. 5. της Πολιτικής Ασφαλείας, «Πολιτική Κωδικών Πρόσβασης».
- Απαγορεύεται σε οποιονδήποτε χρήστη να χρησιμοποιεί για την πρόσβαση στο ΠΣ Αλκυόνη ΙΙ λογαριασμούς ή κωδικούς πρόσβασης, οι οποίοι ανήκουν σε άλλους χρήστες (βλ. και κεφ. 5. της Πολιτικής Ασφαλείας).
- Για να αποφευχθεί η πιθανότητα χρήσης ενός υπηρεσιακού υπολογιστή από μη εξουσιοδοτημένο άτομο (με την «ταυτότητα» ενός άλλου), υποχρεούνται όλοι οι χρήστες Η/Υ να εκτελούν τη λειτουργία shut down μόλις ολοκληρώσουν την εργασία τους.
- Δεν πρέπει να συμπεριλαμβάνουν την είσοδο του κωδικού ασφάλειας σε αυτοματοποιημένες διαδικασίες log-on. Απαγορεύεται η αποθήκευση κωδικών πρόσβασης σε περιηγητές διαδικτύου (browsers).
- Οι μυστικοί κωδικοί πρόσβασης πρέπει να τροποποιούνται από τους χρήστες μετά τη χορήγηση τους ή την επαναφορά τους από τον αρμόδιο διαχειριστή (βλ. και κεφ. 6 της Πολιτικής Ασφαλείας).
- Η πρόσβαση στο Ενιαίο Πληροφοριακό Σύστημα Υποδοχής και Ασύλου «κλειδώνει» αυτόματα μετά από συγκεκριμένη περίοδο αδράνειας. Η ανάκτηση της λειτουργίας και πρόσβασης στην εφαρμογή πραγματοποιείται αφού ο χρήστης πληκτρολογήσει τον προσωπικό του κωδικό.
- Για κάθε χρήστη για τον οποίο ο υπεύθυνος προϊστάμενος αποφασίζει τη χορήγηση πρόσβασης στο Σύστημα συντάσσεται σχετικό έντυπο (βλέπε Παράστημα ΙΙΙ, το οποίο φυλάσσεται με ευθύνη του/της προϊσταμένου/-ης στο αρχείο της Υπηρεσίας. Αντίγραφο του εντύπου δίδεται και στο χρήστη. Το έντυπο αυτό αποτελεί και έγγραφο αποδοχής των υποχρεώσεων, δικαιωμάτων, ευθυνών και περιορισμών του χρήστη βάσει της Πολιτικής Ασφάλειας της ΓΔΠΕ, η οποία διαβιβάζεται στο χρήστη κατά την υπογραφή του εντύπου. Ο λογαριασμός πρόσβασης έχει συγκεκριμένη διάρκεια ισχύος.
- Κάθε χρήστης είναι υπεύθυνος για κάθε είδους ενέργειες - παραλείψεις που αναπτύσσονται στον Η/Υ που χρησιμοποιεί.
- Κάθε χρήστης είναι αποκλειστικά υπεύθυνος για την προστασία των δεδομένων και των αρχείων του από τρίτους. Για το σκοπό αυτό ο χρήστης δύναται να απευθυνθεί στη Γενική Δ/νση Πληροφορικής και Επικοινωνιών για την καλύτερη προστασία ανά περίπτωση.

- Οι υπηρεσιακοί Η/Υ με εγκατεστημένο το σύστημα, μεταξύ των οποίων και Η/Υ που χρησιμοποιούνται από υπαλλήλους φορέων που συνεργάζονται με το ΥΜΑ, χρειάζεται να παραμετροποιούνται και να επιτηρούνται από τη ΓΔΠΕ.
- Η σύνδεση στο Σύστημα πραγματοποιείται αυστηρά και μόνο από δικτυακή υποδομή που ανήκει στο Υ.Μ.Α. (βλ. Κανονισμό Ασφάλειας - Πολιτική Απομακρυσμένης Πρόσβασης).

7. Αρχές επεξεργασίας δεδομένων

Κάθε δραστηριότητα επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να πληροί τις παρακάτω γενικές αρχές:

1. Αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας: Τα δεδομένα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία, με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Η επεξεργασία των προσωπικών δεδομένων πρέπει να θεμελιώνεται σε νόμιμη βάση, άλλως να υπάρχει συγκατάθεση του υποκειμένου των δεδομένων και να είναι απαραίτητη για την επίτευξη έννομου και του δημόσιου συμφέροντος. Όταν η επεξεργασία βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων, κατά τη συλλογή πρέπει να γνωστοποιούνται τα στοιχεία που αναφέρονται στην ενότητα «δικαίωμα ενημέρωσης».
2. Αρχή περιορισμού του σκοπού: Τα δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς.
3. Αρχή της αναλογικότητας: Τα δεδομένα που συλλέγονται και υφίστανται επεξεργασία πρέπει να είναι:
   - συναφή προς το θέμα,
   - πρόσφορα,
   - κατάλληλα για την επίτευξη του σκοπού και
   - αναγκαία (όχι περισσότερα από όσα χρειάζονται) για τους επιδιωκόμενους σκοπούς.
4. Αρχή της ακρίβειας των δεδομένων: Τα δεδομένα πρέπει να είναι ακριβή, να επικαιροποιούνται και να λαμβάνονται τα κατάλληλα μέτρα για την άμεση διόρθωση ανακριβών σε σχέση με τους επιδιωκόμενους σκοπούς επεξεργασίας δεδομένων.
5. Αρχή της ακεραιότητας και εμπιστευτικότητας: Τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλεια και προστασία τους από παράνομη επεξεργασία, απώλεια, καταστροφή ή φθορά τους. Προς τούτο πρέπει να λαμβάνονται κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Τα μέτρα αυτά πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων της επεξεργασίας.
6. Αρχή της χρονικά πεπερασμένης διάρκειας τήρησης: Η χρονική διάρκεια της επεξεργασίας πρέπει να καθορίζεται από το σχεδιασμό της διαδικασίας

επεξεργασίας και τα δεδομένα πρέπει να τηρούνται μόνο για το διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας.

8. Παροχή Δεδομένων σε Τρίτους

Απαγορεύεται οποιαδήποτε παροχή δεδομένων σε τρίτους χωρίς έγγραφη έγκριση τηρουμένης της κείμενης νομοθεσίας και των οδηγιών της Υπηρεσίας που καθορίζει τους σκοπούς της χρήσης των συγκεκριμένων δεδομένων.

Κατά τη μεταφορά/διαβίβαση των δεδομένων εφαρμόζονται τεχνικά και οργανωτικά μέτρα ασφάλειας ανάλογα με τη διαβάθμιση ή τις ειδικές ανάγκες προστασίας της πληροφορίας (π.χ. προσωπικά δεδομένα). Για διαβαθμισμένα δεδομένα τηρούνται οι κανόνες ασφάλειας ανάλογα με το βαθμό διαβάθμισης, ο οποίος πρέπει να αναγράφεται στον ψηφιακό ή οπτικό δίσκο.

Ειδικότερα ως προς την χορήγηση αντιγράφων από το φάκελο αιτούντος, ο/η αιτών/-ούσα έχει δικαίωμα να λαμβάνει, μετά από αίτησή του/της, αντίγραφα των εγγράφων που περιέχονται στο φάκελό του/της και που αφορούν την υπόθεσή του (εκτός αν έχει περιοριστεί η πρόσβαση σε αυτά με απόφαση του/της Προϊσταμένου/-ης). Αντίστοιχο δικαίωμα πρόσβασης έχει και ο δικηγόρος του αιτούντος, σύμφωνα με το άρθ. 76 παρ. 4 του ν. 4939/2022, αλλά και τυχόν άλλοι σύμβουλοι που παρέχουν συνδρομή σε αιτούντες εφόσον τα ζητούμενα στοιχεία σχετίζονται με την παρεχόμενη συνδρομή. Για την άσκηση των παραπάνω δικαιωμάτων απαιτείται εξουσιοδότηση του αιτούντος προς το δικηγόρο ή τον σύμβουλό του με θεώρηση του γνησίου της υπογραφής του/της αιτούντος/-σας από τα αρμόδια κατά νόμο όργανα. Όσον αφορά στη συνέντευξη, το επίσημο πρακτικό είναι το ηχητικό αρχείο. Παράλληλα, τηρείται πλήρες πρακτικό από τους χειριστές/-ριες το οποίο αποτελεί στοιχείο του διοικητικού φακέλου του αιτούντος και ως εκ τούτου ο αιτών ή συνήγορός του νομιμοποιείται να ζητήσει αντίγραφο του πρακτικού.

Ως εκ τούτου: α) Αν κάποιος αιτηθεί αντίγραφο του πρακτικού θα πρέπει να ερωτηθεί εάν θέλει το ηχητικό αρχείο ή το "πρακτικό", β) Σε περίπτωση που ζητά να λάβει αντίγραφο του "πρακτικού", εκτυπώνεται αυτό που έχει αναρτηθεί στην «Αλκυόνη» και χορηγείται ως ακριβές αντίγραφο, γ) Σε περίπτωση που ζητά να λάβει αντίγραφο του ηχητικού αρχείου, θα πρέπει να του ζητείται ψηφιακός δίσκος εγγραφής (CD), ώστε ο αρμόδιος υπάλληλος να αντιγράψει το αρχείο, δ) Σε περίπτωση που ζητηθεί οποιοδήποτε άλλο έγγραφο από το φάκελο του αιτούντος, χορηγείται σε κάθε περίπτωση εκτός εάν πρόκειται για έγγραφο που αφορά φορολογικό απόρρητο ή ιδιωτική κι οικογενειακή ζωή τρίτου ή εάν, με απόφαση του/της Προϊσταμένου/-ης ΠΓΑ/ΑΚΑ, θεωρείται αιτιολογημένα ότι θα δυσχεράνει σοβαρά έρευνες δικαστικών, διοικητικών, αστυνομικών ή στρατιωτικών αρχών σχετικά με την τέλεση εγκλήματος ή διοικητικής παράβασης.

9. Προστασία Προσωπικών Δεδομένων

Ως προσωπικό δεδομένο θεωρείται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο (έμμεσα ή άμεσα) φυσικό πρόσωπο (υποκείμενο των δεδομένων), συμπεριλαμβανομένων των κατηγοριών που χρήζουν μεγαλύτερης προστασίας, όπως τα γενετικά και βιομετρικά δεδομένα.

Κάθε χρήστης του πληροφοριακού συστήματος Αλκυόνη ΙΙ οφείλει να επεξεργάζεται τα απολύτως απαραίτητα προσωπικά δεδομένα για το σκοπό που έχει οριστεί στο πλαίσιο των υπηρεσιακών του καθηκόντων. Απαγορεύεται οποιαδήποτε άλλη αποθήκευση ή πρόσβαση σε προσωπικά δεδομένα.

Ως περιστατικό παραβίασης προσωπικών δεδομένων νοείται κάθε συμβάν στο οποίο πραγματοποιείται τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία. Σε περίπτωση υποψίας περιστατικού παραβίασης προσωπικών δεδομένων ο υπάλληλος υποχρεούται να ενημερώσει άμεσα τον Προϊστάμενο της Υπηρεσίας και τη Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών/Υ.Μ.Α., ακολουθώντας τη διαδικασία αναγγελίας περιστατικών ασφάλειας.

Η πρόσβαση σε ακατέργαστα δεδομένα (raw data) παρέχεται στο προσωπικό σύμφωνα με την διαβάθμιση ρόλων που έχει πραγματοποιηθεί, εντούτοις η δυνατότητα εξαγωγής των εν λόγω δεδομένων από το Πληροφοριακό Σύστημα Αλκυόνη ΙΙ είναι αυστηρά περιορισμένη και επιτρέπεται μόνο στα εξουσιοδοτημένα στελέχη της ΓΔΠΕ για σκοπούς ασφάλειας, συντήρησης, ελέγχου, επεξεργασίας και ανάλυσης. Για το σκοπό αυτό, απαγορεύεται η χρήση ή η ενσωμάτωση οποιασδήποτε λειτουργίας εντός του Πληροφοριακού Συστήματος Αλκυόνη ΙΙ που να επιτρέπει την εξαγωγή ακατέργαστων δεδομένων σε μορφή επεξεργάσιμη (πχ csv, xlsx) από μη εξουσιοδοτημένους χρήστες.

Σε περίπτωση που υφίστανται ειδικές ανάγκες που απαιτούν την εξαγωγή των ακατέργαστων δεδομένων από μη εξουσιοδοτημένα στελέχη ή την παροχή τέτοιων δεδομένων σε τρίτους, είτε εντός είτε εκτός του Υπουργείου, θα πρέπει να υποβάλλεται επίσημο και αιτιολογημένο αίτημα προς τη ΓΔΠΕ. Το εν λόγω αίτημα θα υπόκειται σε αξιολόγηση βάσει της σημασίας, της επείγουσας ανάγκης και των πιθανών κινδύνων ασφαλείας που μπορεί να συνεπάγεται η εν λόγω πρόσβαση. Σε περίπτωση έγκρισης, θα καθορίζονται συγκεκριμένοι όροι χρήσης και προστασίας των δεδομένων, προκειμένου να ελαχιστοποιείται ο κίνδυνος διαρροής ή κατάχρησης.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ: ΕΝΤΥΠΟ ΠΡΟΣΒΑΣΗΣ ΣΤΟ ΕΝΙΑΙΟ Π.Σ. ΥΠΟΔΟΧΗΣ ΚΑΙ ΑΣΥΛΟΥ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Μετανάστευσης & Ασύλου

Αίτηση πρόσβασης υπαλλήλων του Υπουργείου Μετανάστευσης και Ασύλου, σύμφωνα με την Πολιτική Ασφαλείας της Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών του Υπουργείου Μετανάστευσης και Ασύλου, όπως ισχύει.

ΣΤΟΙΧΕΙΑ ΥΠΑΛΛΗΛΟΥ- ΧΡΗΣΤΗ	
Υπηρεσία πχ. ΠΓΑ/ΑΚΑ, ΔΟΜΗ, ΤΜΗΜΑ, ΔΙΕΥΘΥΝΣΗ	
Διεύθυνση/ Τ.Κ.:	
Όνομα Υπαλλήλου:	
Επώνυμο Υπαλλήλου:	
Α.Δ.Τ. / Διαβατήριο:	
Οργανική Μονάδα:	
Τηλ. Επικοινωνίας:	
Υπηρεσιακό email επικοινωνίας:	

ΣΤΟΙΧΕΙΑ ΠΡΟΣΒΑΣΗΣ **(συμπληρώνεται από Προϊστάμενο/-η)**	
Αιτιολόγηση άδειας πρόσβασης:	
Δικαιώματα πρόσβασης:	
Είδος συσκευής (Η/Υ σταθερός, φορητός/ προσωπικός, υπηρεσιακός):	Υπηρεσιακός Ηλεκτρονικός Υπολογιστής ή υπηρεσιακό laptop

Με το παρόν δηλώνω ότι αποδέχομαι και δεσμεύομαι από τους όρους της Πολιτικής Ασφαλείας της Γενικής Διεύθυνσης Πληροφορικής και Επικοινωνιών και οφείλω να σέβομαι τα δικαιώματα και τους περιορισμούς που απορρέουν από τη συγκεκριμένη πολιτική.

Με το παρόν αποδίδονται στον/-ην ανωτέρω το δικαίωμα ασφαλούς πρόσβασης στο ΠΣ «Αλκυόνη ΙΙ» του Υπουργείου Μετανάστευσης και Ασύλου.

Υπογραφή Υπαλλήλου:	Υπογραφή Προϊσταμένου:
Ονοματεπώνυμο: Ημερομηνία:	Ονοματεπώνυμο: Ημερομηνία:

Επισημαίνεται ότι η χρήση των πληροφοριών που προκύπτουν από την πρόσβαση στην εν λόγω εφαρμογή επιτρέπεται μόνο για τον σκοπό για τον οποίο έχει εκχωρηθεί το δικαίωμα πρόσβασης.

Το παρόν έντυπο διακινείται μέσω του Συστήματος Ηλεκτρονικής Διακίνησης Εγγράφων ΙΡΙΔΑ 2, και υπογράφεται από τον άμεσα προϊστάμενο του υπηρετούντος.

ΠΑΡΑΡΤΗΜΑ IV: ΦΥΛΛΑΔΙΟ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗΣ ΕΡΓΑΖΟΜΕΝΩΝ ΣΧΕΤΙΚΑ ΜΕ ΤΑ ΠΕΡΙΣΤΑΤΙΚΑ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

1. Τι είναι η παραβίαση δεδομένων προσωπικού χαρακτήρα

Ένα περιστατικό παραβίασης προσωπικών δεδομένων συντελείται όταν τα προσωπικά δεδομένα για τα οποία το ΥΜΑ είναι υπεύθυνο, όπως στοιχεία επωφελούμενων των παρεχόμενων υπηρεσιών (πχ. αιτούντων και δικαιούχων διεθνή προστασία, αιτούντων και δικαιούχων προσωρινή προστασία, αιτούντων και δικαιούχων αδειών διαμονής πολιτών Τρίτων Χωρών, αιτούντων αδειών διαμονής Επενδυτών πολιτών Τρίτων Χωρών), , εργαζομένων, υποψηφίων εργαζομένων, συνεργαζόμενων φορέων και προμηθευτών (που είναι φυσικά πρόσωπα) δημοσιοποιούνται, τυχαία ή παράνομα, σε μη εξουσιοδοτημένα πρόσωπα, καθίστανται, προσωρινά ή μόνιμα, μη διαθέσιμα ή αλλοιώνονται.

Βασικά στοιχεία της παραβίασης δεδομένων προσωπικού χαρακτήρα είναι τα ακόλουθα:

- ✓ η παραβίαση της ασφάλειας που οδηγεί σε καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση σε δεδομένα προσωπικού χαρακτήρα (άρθρο 4 στοιχείο 12 ΓΚΠΔ),
- ✓ η παραβίαση της ασφάλειας έχει επίπτωση στα προσωπικά δεδομένα και μπορεί να λάβει χώρα είτε τυχαία είτε παράνομα,
- ✓ η παραβίαση αυτή έχει μπορεί να έχει δυσμενείς επιπτώσεις στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων,
- ✓ η παραβίαση αυτή επιφέρει υποχρεώσεις του ΥΜΑ βάσει του ΓΚΠΔ έναντι της εποπτικής αρχής και των θιγόμενων προσώπων αναλόγως του επιπέδου κινδύνου.

2. Ποια είναι τα είδη παραβίασης δεδομένων προσωπικού χαρακτήρα

- ✓ Παραβίαση της εμπιστευτικότητας (confidentiality): συντελείται όταν υπάρχει αποκάλυψη των προσωπικών δεδομένων σε μη εξουσιοδοτημένα πρόσωπα.
- ✓ Παραβίαση της ακεραιότητας (integrity): συντελείται όταν υπάρχει αλλοίωση ή παραποίηση των προσωπικών δεδομένων.
- ✓ Παραβίαση της διαθεσιμότητας (availability): συντελείται όταν τα προσωπικά δεδομένα παύουν να είναι στη διάθεση των εξουσιοδοτημένων χρηστών όποτε απαιτείται η χρήση τους - υπάρχει απώλεια της πρόσβασης ή καταστροφή των προσωπικών δεδομένων.

3. Ποιες είναι οι πιθανές επιπτώσεις ενός περιστατικού παραβίασης στα φυσικά πρόσωπα

Μια παραβίαση μπορεί δυνητικά να έχει διάφορες σημαντικές δυσμενείς συνέπειες στα φυσικά πρόσωπα, οι οποίες μπορούν να οδηγήσουν σε σωματική, υλική ή ηθική βλάβη. Αυτή η βλάβη μπορεί να περιλαμβάνει απώλεια του ελέγχου επί των δεδομένων τους, περιορισμό των δικαιωμάτων τους, διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, παράνομη άρση της ψευδωνυμοποίησης, βλάβη της φήμης και απώλεια της εμπιστευτικότητας των δεδομένων προστατεύονται από επαγγελματικό απόρρητο. Μπορεί επίσης να περιλαμβάνει οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα γι' αυτά τα πρόσωπα.

4. Ποιες είναι οι βασικές υποχρεώσεις του φορέα μου σε περίπτωση που λάβει χώρα περιστατικό παραβίασης προσωπικών δεδομένων

- ✓ Το ΥΜΑ οφείλει, μόλις αποκτήσει γνώση του περιστατικού παραβίασης, να αξιολογήσει άμεσα την σοβαρότητά του και καθώς και τις συνέπειες και τα δυσμενή αποτελέσματά του για τα φυσικά πρόσωπα.
- ✓ Το ΥΜΑ οφείλει να λάβει αμέσως μέτρα για την αντιμετώπιση και περιορισμό της παραβίασης καθώς και μέτρα διόρθωσης του προβλήματος και αποφυγής παρόμοιων παραβιάσεων στο μέλλον.
- ✓ **Υποχρέωση υποβολής γνωστοποίησης στην Αρχή:** Εάν το περιστατικό παραβίασης θέτει σε **κίνδυνο** τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, το ΥΜΑ οφείλει να υποβάλει γνωστοποίηση στην Αρχή αμέσως ή το αργότερο εντός 72 ωρών αφότου αντιληφθεί το περιστατικό.
- ✓ **Υποχρέωση ενημέρωσης των επηρεαζόμενων προσώπων:** Εάν το περιστατικό παραβίασης δημιουργεί **υψηλό κίνδυνο** για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, το ΥΜΑ οφείλει επιπλέον της γνωστοποίησης να ενημερώσει σχετικά τα επηρεαζόμενα πρόσωπα με πρόσφορο και κατανοητό τρόπο αμελλητί (δηλαδή σε χρόνο μικρότερο των 72 ωρών).
- ✓ **Υποχρέωση τήρησης εσωτερικού μητρώου:** Σε κάθε περίπτωση, το ΥΜΑ οφείλει να καταγράψει και τεκμηριώσει κάθε περιστατικό, ανεξαρτήτως του επιπέδου κινδύνου, σε εσωτερικό μητρώο.

5. Ποια είναι τυπικά παραδείγματα περιστατικών παραβίασης που ενδέχεται να επηρεάσουν τον οργανισμό

- ✓ Αποστολή ηλεκτρονικού μηνύματος με προσωπικά δεδομένα πολιτών, ή εργαζομένων, ή δικαιούχων, κ.λπ. σε λάθος παραλήπτη.
- ✓ Αστοχία υλικού και διακοπή της λειτουργίας του πληροφοριακού συστήματος.
- ✓ Κλοπή του αντιγράφου ασφαλείας της βάσης δεδομένων.
- ✓ Κλοπή εγγράφων με προσωπικά δεδομένα από γραφείο ή ξεκλείδωτο φωριαμό.
- ✓ Κλοπή ή απώλεια φορητού υπολογιστή/συσκευής (π.χ. USB stick) με προσωπικά δεδομένα.
- ✓ Μόλυνση από κακόβουλο λογισμικό με αποτέλεσμα την παράνομη διαβίβαση αρχείων με προσωπικά δεδομένα σε τρίτους.
- ✓ Τυχαία διαγραφή προσωπικών δεδομένων από την βάση δεδομένων.
- ✓ Εξαγωγή δεδομένων από διαδικτυακό τόπο με επίθεση SQL Injection.
- ✓ Εξαπάτηση εργαζομένου με αποτέλεσμα την ανακοίνωση προσωπικών δεδομένων σε κακόβουλα πρόσωπα.

6. Πως μπορώ να διακρίνω ένα πιθανό περιστατικό παραβίασης

Ένα περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα σχετίζεται με τα προσωπικά δεδομένα που συλλέγει και επεξεργάζεται το ΥΜΑ για να επιτελέσει τις δραστηριότητές του. Συνεπώς, το περιστατικό θα αφορά τα δεδομένα κάποιας κατηγορίας φυσικών προσώπων όπως επωφελούμενων των παρεχόμενων υπηρεσιών, εργαζόμενων, υποψηφίων εργαζομένων, συνεργαζόμενων φορέων και προμηθευτών φυσικών προσώπων ή άλλων κατηγοριών.

Το περιστατικό παραβίασης επιφέρει πλήγμα στην ασφάλεια των προσωπικών δεδομένων όπως καταστροφή ή απώλεια των δεδομένων, αποκάλυψη αυτών ή απόκτηση πρόσβασης σε αυτά από μη εξουσιοδοτημένα πρόσωπα ή αλλοίωση των δεδομένων.

Επειδή κάθε περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα αποτελεί συμβάν ασφαλείας (security incident) το οποίο επηρεάζει τα προσωπικά δεδομένα, καλό είναι ο εργαζόμενος να ενημερώνει τα αρμόδια πρόσωπα του ΥΜΑ (cert@migration.gov.gr) για κάθε ζήτημα ασφάλειας χωρίς να συνδέεται εμφανώς με προσωπικά δεδομένα όπως αν διαπιστώσει μόλυνση του υπολογιστή του ή της φορητής συσκευής από ιομορφικό λογισμικό, παράνομη εγκατάσταση προγραμμάτων ή εφαρμογών, δυσλειτουργία του ηλεκτρονικού του υπολογιστή κλπ.

7. Τι ενέργειες μπορώ να κάνω εάν αντιληφθώ πιθανό περιστατικό παραβίασης

- ✓ Να ενημερώσω αμέσως τα αρμόδια πρόσωπα του οργανισμού (cert@migration.gov.gr) σχετικά με το πιθανό περιστατικό παραβίασης, σύμφωνα με την αντίστοιχη πολιτική, ή/και τον Υπεύθυνο Προστασίας Δεδομένων (dpo@migration.gov.gr). Σε κάθε περίπτωση, μπορεί να ενημερωθεί η Γενική Διεύθυνση Πληροφορικής και Επικοινωνιών (dg.ict@migration.gov.gr).
- ✓ Να διακόψω προσωρινά τυχόν επεξεργασία προσωπικών δεδομένων που επηρεάζεται από το περιστατικό παραβίασης.
- ✓ Να συγκεντρώσω, αν είναι εφικτό, ό,τι στοιχεία σχετίζονται με αυτό χωρίς να τα αλλοιώσω ή καταστρέψω.
- ✓ Να συνδράμω τα αρμόδια πρόσωπα στην διερεύνηση του περιστατικού με πληροφορίες που τυχόν γνωρίζω σχετικά με αυτό ή σχετικά με τα χαρακτηριστικά και τον τρόπο επεξεργασίας των δεδομένων που αφορά.

8. Τι ενέργειες μπορώ να κάνω για να προστατέψω τα δεδομένα που χειρίζομαι από πιθανό περιστατικό παραβίασης

- ✓ Να μην αφήνω έκθετα έγγραφα στο γραφείο μου και στους φωριαμούς που έχω πρόσβαση.
- ✓ Να ελέγχω τις διευθύνσεις των παραληπτών των μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- ✓ Να μην αποθηκεύω προσωπικά δεδομένα σε φορητές συσκευές χωρίς κρυπτογράφηση.
- ✓ Να μην αποθηκεύω δεδομένα στον προσωπικό μου υπολογιστή μετά το πέρας της τηλεργασίας εκτός αν είναι κρυπτογραφημένα.
- ✓ Να γνωρίζω και εφαρμόζω τις πολιτικές της εταιρείας μου.
- ✓ Να τηρώ τα δεδομένα που χειρίζομαι με εμπιστευτικότητα.
- ✓ Να επιλέγω κατάλληλο συνθηματικό, να μην το γνωστοποιώ σε άλλους και να το αλλάζω σε τακτική βάση.
- ✓ Να μην διακινώ με κανένα τρόπο λίστες με προσωπικά δεδομένα (αρχεία csv, excel, κ.λπ.).
- ✓ Να μην εξάγω αρχεία (csv, excel, κ.λπ.) με προσωπικά δεδομένα από τα πληροφοριακά συστήματα του οργανισμού.

ΠΑΡΑΡΤΗΜΑ V: ΔΗΛΩΣΗ ΤΗΡΗΣΗΣ ΑΠΟΡΡΗΤΟΥ

Ο/Η υπογράφων / ουσα ..... κάτοικος ....., οδός ....., κάτοχος του υπ' αριθμ. ..... Α.Δ.Τ. με την ιδιότητα του εντεταλμένου υπαλλήλου από την/ον ..... (*συμπληρώνεται κατά περίπτωση ο εντέλλων Φορέας, π.χ. Εθνική Αρχή Διαφάνειας, Αρχή Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες, κλπ.*) βάσει της οποίας μου παρέχεται δικαίωμα πρόσβασης σε εμπιστευτικά δεδομένα και δεδομένα προσωπικού χαρακτήρα, τα οποία περιέχονται σε πληροφοριακά συστήματα και σε συστήματα και μέσα αρχειοθέτησης του Υπουργείου Μετανάστευσης και Ασύλου.

Δηλώνω υπεύθυνα ότι:

1. Αναλαμβάνω την υποχρέωση να μην αποκαλύπτω, κοινοποιώ, διαθέτω πληροφορίες, εμπιστευτικού χαρακτήρα ή να επιτρέπω ή να καθιστώ δυνατή την πρόσβαση οποιουδήποτε τρίτου άμεσα ή έμμεσα την κοινοποίηση ή δημοσιοποίηση εμπιστευτικών πληροφοριών σε οποιονδήποτε τρίτο. Η υποχρέωση αυτή ισχύει με την επιφύλαξη της εφαρμογής διάταξης νόμου που επιτάσσει την αποκάλυψη των εν λόγω πληροφοριών.
2. Να μην χρησιμοποιώ πληροφορίες για θέματα που χαρακτηρίζονται από τις κείμενες διατάξεις ως απόρρητα, καθώς και σε κάθε περίπτωση που τούτο επιβάλλεται από την κοινή πείρα και λογική για γεγονότα ή πληροφορίες που κατέχω λόγω της υπηρεσίας ή της θέσης μου, και δεν επιτρέπω την αθέμιτη χρήση τους για να εξυπηρετηθεί οποιοδήποτε συμφέρον, δημόσιο ή ιδιωτικό. - [Ν. 3528/2007 άρθρο 26, Ν. 3528/2007, άρθρο 107 παρ. 1 περ. η, όπως αντικαταστάθηκε από το άρθρο δεύτερο του Ν. 4057/2012 και ΠΚ άρθρο 252]
3. Με τον όρο Εμπιστευτικές Πληροφορίες, όπως αυτός χρησιμοποιείται στην παρούσα δήλωση, νοούνται όλες οι πληροφορίες, τα στοιχεία, οι μέθοδοι, οι πολιτικές και οι διαδικασίες που αφορούν στην οργάνωση, τη διοίκηση, τον αναπτυξιακό σχεδιασμό, την τεχνογνωσία, τα συστήματα και μέσα που περιέχουν Εμπιστευτικές Πληροφορίες.
4. Ως εμπιστευτική πληροφορία νοείται επίσης και κάθε δεδομένο προσωπικού χαρακτήρα, δηλαδή κάθε πληροφορία που μπορεί να αφορά ένα πρόσωπο, η ταυτότητα του οποίου είναι γνωστή ή μπορεί να προσδιοριστεί. Τα δεδομένα αυτά μπορεί να αναφέρονται σε άλλους εργαζόμενους/ απασχολούμενους στο ΥΜΑ, σε πρόσωπα με τα οποία συναλλάσσεται ή συνεργάζεται το ΥΜΑ ή πρόσωπα, τα δεδομένα των οποίων περιέχονται σε αρχεία, σε στοιχεία του κοινού, σε στοιχεία πολιτών που επικοινωνούν με το ΥΜΑ και υπόκεινται σε επεξεργασία στο πλαίσιο των διαδικασιών δημιουργίας περιεχομένου και των διοικητικών δραστηριοτήτων του ΥΜΑ.
5. Δεν δημοσιοποιώ πληροφορίες που αφορούν την ιδιωτική και οικογενειακή ζωή των πολιτών (ή άλλα ευαίσθητα προσωπικά δεδομένα), τις οποίες κατέχω λόγω της υπηρεσιακής μου θέσης. - [Ν. 2690/1999 άρθρο 5 παρ. 3 (ΚΔΔ, ΦΕΚ 102 Α) και Ν. 4624/2019 (ΦΕΚ 137 Α)]

6. Οι εμπιστευτικές πληροφορίες μπορεί να περιέχονται σε πληροφοριακά συστήματα, φορητά αποθηκευτικά μέσα, υλικούς φορείς ήχου ή εικόνας, δισκέτες ή ψηφιακούς δίσκους ηλεκτρονικών υπολογιστών, μηχανές, πρωτότυπα κάθε είδους και εφαρμογής, σχέδια, ορισμούς και επεξηγήσεις, είδη οιασδήποτε κατασκευής, έγγραφα αναγνώσιμα από μηχανές ή τον άνθρωπο ή και να έχουν χαρακτήρα προφορικής δήλωσης.
7. Να φροντίζω να διασφαλίζω την εμπιστευτικότητα των πληροφοριών που χειρίζομαι σε κάθε περίπτωση, και ιδιαίτερα όταν χρησιμοποιώ νέες τεχνολογίες πληροφορικής και επικοινωνίας. - [Ν. 3528/2007 άρθρο 26 (ΥΚ, ΦΕΚ 26 Α)]
8. Κατά τη διάρκεια διενέργειας της εντελλόμενης διαδικασίας, αλλά και μετά το πέρας αυτής, εις το διηνεκές, δεν θα αποκαλύπτω, συζητώ, ανταλλάσσω ή μεταβιβάζω τα στοιχεία (ή μέρος των στοιχείων), καθ' οιονδήποτε τρόπο (άμεσο ή έμμεσο) και υπό οιαδήποτε μορφή σε (με) τρίτους, παρά μόνο σε (με) αυτούς που ρητά αναφέρονται στην εντελλόμενη διαδικασία ότι θα έχουν πρόσβαση.
9. Κατά τη διάρκεια διενέργειας της εντελλόμενης διαδικασίας, αλλά και μετά το πέρας αυτής, εις το διηνεκές, δεν θα δημοσιοποιώ ή διαθέτω με οποιονδήποτε τρόπο αποτελέσματα της έρευνας που μπορεί να οδηγήσουν εμμέσως στην αποκάλυψη προσωπικών δεδομένων.

Με την υπογραφή αυτής της Δήλωσης, βεβαιώνω ότι έχω διαβάσει και κατανοήσει και αποδέχομαι ανεπιφύλακτα ότι οι παραπάνω υποχρεώσεις αφορούν όλες τις Εμπιστευτικές Πληροφορίες καθώς και τα προσωπικά δεδομένα, ανεξαρτήτως της μεθόδου και του μέσου με τα οποία θα αποκτήσω πρόσβαση σε αυτά και ανεξαρτήτως του είδους επεξεργασίας.

, ……/……/2024

Ο/Η Δηλ……..

ΠΑΡΑΡΤΗΜΑ VI: ΕΝΤΥΠΟ ΑΠΟΔΟΧΗΣ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

	ΕΝΤΥΠΟ ΑΠΟΔΟΧΗΣ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Ονομασία Υπηρεσίας	

Τόπος: ……., Ημερομηνία:…../…./…..

Ο/Η υπογεγραμμένος/η

Α.Μ. …….,

ΕΠΩΝΥΜΟ ……,

ΟΝΟΜΑ ……..,

ΠΑΤΡΩΝΥΜΟ ……,

αποδέχομαι τις υποχρεώσεις, δικαιώματα, ευθύνες και περιορισμούς όπως αυτά ορίζονται στις Πολιτικές Ασφάλειας του Υπουργείου Μετανάστευσης και Ασύλου.

Ο/Η Χρήστης

Ο/Η Διευθυντής/τρία / Προϊστάμενος/η
της Υπηρεσίας

(ονοματεπώνυμο & υπογραφή)