ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΕΞΩΤΕΡΙΚΩΝ ΧΡΗΣΤΩΝ ΤΗΣ ΕΘΝΙΚΗΣ ΑΡΧΗΣ ΣΤΟΙΧΗΜΑΤΩΝ

ΙΣΤΟΡΙΚΟ ΤΡΟΠΟΠΟΙΗΣΗΣ ΠΟΛΙΤΙΚΗΣ

Αριθμός έκδοσης	Ημερομηνία	Τροποποίηση από	Λόγοι Τροποποίησης
V1	22/02/2022	-	-
V2	23/03/2022	Λειτουργό ΤΠ	Προσθήκη "ΜΕΡΟΣ 12 – ΑΝΑΦΟΡΑ ΠΑΡΑΒΙΑΣΕΩΝ ΑΣΦΑΛΕΙΑΣ"
V3	21/04/2022	Λειτουργό Συμμόρφωσης	Διόρθωση αρίθμησης στα (πρώην) Μέρη 13 μέχρι 17 & Διαγραφή αναφοράς σε εσωτερική διαδικασία στο 12.1
V4	08/03/2023	Λειτουργό Συμμόρφωσης και αρμόδιους λειτουργούς	Τροποποιήσεις προς βελτίωση: • ΜΕΡΟΣ 8 – ΠΟΛΙΤΙΚΗ ΚΩΔΙΚΟΥ ΠΡΟΣΒΑΣΗΣ • ΜΕΡΟΣ 14 –ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΡΟΜΗΘΕΥΤΩΝ/ΠΩΛΗΤΩΝ • ΜΕΡΟΣ 17 – ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΗΣ • ΜΕΡΟΣ 18 – ΕΦΑΡΜΟΓΗ ΠΟΛΙΤΙΚΗΣ
V5	29/03/2023	Λειτουργό Συμμόρφωσης και αρμόδιους λειτουργούς	Τροποποιήσεις προς βελτίωση: • ΜΕΡΟΣ 17 – ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΗΣ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΜΕΡΟΣ 1 - ΕΙΣΑΓΩΓΗ

Το παρόν έγγραφο Πολιτικής Ασφάλειας Πληροφοριών αποτελείται από μία σειρά κανονισμών που έχουν θεσπιστεί από τη διοίκηση της Εθνικής Αρχής Στοιχημάτων (Αρχή) με σκοπό να διασφαλίσουν ότι, οι εμπλεκόμενοι εξωτερικοί φορείς και τα δίκτυα που σχετίζονται με τον οργανισμό πληρούν τις σχετικές προϋποθέσεις που αφορούν την ασφάλεια πληροφοριών και την προστασία δεδομένων. Ο ιδιοκτήτης (Owner) της Πολιτικής Ασφάλειας Πληροφοριών είναι η Εθνική Αρχή Στοιχημάτων.

ΜΕΡΟΣ 2 - ΟΡΙΣΜΟΙ

ΤΠ: Τεχνολογία Πληροφορικής

Εξωτερικοί Χρήστες: εξωτερικοί συνεργάτες της Αρχής και μέλη του προσωπικού αυτών, κρατικές υπηρεσίες, δημόσιες αρχές, διωκτικές αρχές και εμπλεκόμενα με την Αρχή μέρη. Τα μέλη του προσωπικού της Αρχής, ο Πρόεδρος και τα μέλη του Διοικητικού Συμβουλίου της, εσωτερικοί και εξωτερικοί σύμβουλοι που χρησιμοποιούν της εγκαταστάσεις και εξοπλισμό της Αρχής, διέπονται από την Πολιτική Ασφάλειας Πληροφοριών της Αρχής, η οποία καθορίζεται σε ξεχωριστό, εκτενέστερο έγγραφο.

ΜΕΡΟΣ 3 – ΒΑΣΙΚΕΣ ΑΡΧΕΣ

3.1 Τα Συστήματα Τεχνολογιών Πληροφορικής (“ΤΠ”) πρέπει να προστατεύονται διαρκώς από μη εξουσιοδοτημένη πρόσβαση.

3.2 Τα Συστήματα ΤΠ πρέπει να είναι συμβατά με τις σχετικές Πολιτικές και Διαδικασίες της Αρχής.

3.3 Η Αρχή διασφαλίζει ότι, οι Εξωτερικοί Χρήστες είναι ενήμεροι και δηλώνουν (γραπτώς ή ηλεκτρονικά) ότι έχουν διαβάσει και κατανοήσει την Πολιτική Ασφάλειας Πληροφοριών Εξωτερικών Χρηστών της Εθνικής Αρχής Στοιχημάτων, καθώς και άλλες σχετικές Πολιτικές.

3.4 Τα δεδομένα που βρίσκονται αποθηκευμένα στα Συστήματα ΤΠ πρέπει να τυγχάνουν ασφαλούς διαχείρισης σύμφωνα με τους υφιστάμενους νόμους προστασίας δεδομένων (συμπεριλαμβανομένου του γενικού κανονισμού για την προστασία δεδομένων της Ε.Ε. (ΓΚΠΔ)).

3.5 Πρόσβαση σε πληροφορίες και/ή συστήματα πληροφοριών δίνεται στη βάση «ανάγκης πρόσβασης» και «περιορισμένων δικαιωμάτων», αναλόγως των καθηκόντων των χρηστών.

3.6 Εφαρμόζονται όλοι οι σχετικοί τεχνικοί και/ή οργανωτικοί έλεγχοι για να διασφαλιστεί ότι όλα τα δεδομένα, είτε σε ψηφιακή είτε σε έντυπη μορφή, προστατεύονται από τυχόν διαρροή πληροφοριών και/ή παράτυπη χρήση.

3.7 Οποιαδήποτε παραβίαση ασφάλειας που σχετίζεται με τα Συστήματα ΤΠ ή με δεδομένα που είναι αποθηκευμένα σε αυτά, καταγγέλλεται από τους Εξωτερικούς Χρήστες προς την Αρχή και διερευνάται από το Τμήμα ΤΠ της Αρχής, σύμφωνα με τις εσωτερικές διαδικασίες.

Σε περίπτωση που υπάρχει υποψία, υπόνοια ή γνώση ότι πιθανή παραβίαση αφορά προσωπικά δεδομένα, ενημερώνεται και ο Λειτουργός Προστασίας Δεδομένων της Αρχής.

3.8 Οι Εξωτερικοί Χρήστες πρέπει να δηλώνουν κάθε υποψία που αφορά την ασφάλεια σε σχέση με τα Συστήματα ΤΠ ή τα αποθηκευμένα δεδομένα στο Τμήμα ΤΠ της Αρχής. Σε περίπτωση που υπάρχει υποψία, υπόνοια ή γνώση ότι πιθανή παραβίαση αφορά προσωπικά δεδομένα, θα πρέπει να ενημερώνεται και ο Λειτουργός Προστασίας Δεδομένων της Αρχής.

3.9 Οι συσκευές που παρέχονται από την Αρχή σε Εξωτερικούς Χρήστες χρησιμοποιούνται αποκλειστικά για εργασία που αφορά την Αρχή.

ΜΕΡΟΣ 4 – ΡΟΛΟΙ ΚΑΙ ΕΥΘΥΝΕΣ

4.1 Εξωτερικοί Χρήστες

Οι Εξωτερικοί Χρήστες έχουν την ευθύνη για τη διασφάλιση ότι:

α) είναι ενήμεροι για τις πολιτικές ασφάλειας πληροφοριών, τις διαδικασίες και τις ευθύνες Χρήσης που ισχύουν στον τομέα της εργασίας τους,
β) είναι ενήμεροι για τις προσωπικές τους ευθύνες για την ασφάλεια των πληροφοριών,
γ) έχουν την απαιτούμενη εκπαίδευση για τα συστήματα που χρησιμοποιούν,
δ) γνωρίζουν πώς να ζητούν καθοδήγηση/βοήθεια σε θέματα ασφάλειας πληροφοριών,
ε) τα Συστήματα τους που τυγχάνουν χρήσης από τρίτο μέρος και περιλαμβάνουν πληροφορίες της Αρχής, έχουν αξιολογηθεί ως κατάλληλα και συμμορφώνονται με τις προϋποθέσεις ασφάλειας της Αρχής,
στ) έχουν επίγνωση των όρων της παρούσας Πολιτικής, της σχετικής νομοθεσίας και κανονισμών,
ζ) γίνεται αναφορά στην Αρχή, όπου απαιτείται, όσον αφορά σε θέματα ασφάλειας ή δυσλειτουργιών που προκύπτουν ή συμπίπτουν με τις ευθύνες τους,
η) υπάρχει διαρκής συμμόρφωση τους με όλα τα σχετικά πεδία της παρούσας Πολιτικής κατά τη χρήση των Συστημάτων της Αρχής,
θ) σε καμία περίπτωση δεν επιτρέπεται να χρησιμοποιήσουν εξωτερικό μέσο (π.χ. stick USB ή οποιοδήποτε είδος δίσκου) για τη μεταφορά αρχείων στα Συστήματα ΤΠ της Αρχής,
ι) η χρήση των πόρων της Αρχής γίνεται με τρόπο υπεύθυνο και με αυστηρή αποχή από τις ακόλουθες δραστηριότητες:
    - πρόκληση βλάβης ή απόπειρα πρόκλησης βλάβης σε σύστημα πληροφοριών,
    - προσπάθεια πρόσβασης σε πηγή πληροφοριών για την οποία δεν κατέχουν δικαίωμα πρόσβασης,
    - εισαγωγή ή απόπειρα εισαγωγής κακόβουλου κώδικα σε σύστημα πληροφοριών (π.χ. ιό, Δούρειο Ίππο, κλπ.),
    - παράβαση ή απόπειρα παράβασης των κανόνων χρήσης ή της άδειας χρήσης οποιουδήποτε προϊόντος λογισμικού χρησιμοποιείται από την Αρχή.

4.2 Ασφάλεια πληροφοριών σε έργα

α. Η ασφάλεια δεδομένων είναι αναπόσπαστο κομμάτι στις διαδικασίες της Εθνικής Αρχής Στοιχημάτων, για να διασφαλίζεται ότι οι κίνδυνοι ασφάλειας πληροφοριών εντοπίζονται και αντιμετωπίζονται. Οι μέθοδοι διαχείρισης έργων της Αρχής διασφαλίζουν ότι:

- ο σκοπός της ασφάλειας πληροφοριών περιλαμβάνεται στους στόχους έργου,
- πραγματοποιείται αξιολόγηση ρίσκου ασφάλειας πληροφοριών στα αρχικά στάδια του έργου για να καθοριστούν οι κατάλληλοι έλεγχοι,
- η ασφάλεια δεδομένων είναι μέρος όλων των σταδίων της μεθοδολογίας έργου που εφαρμόζεται.

β. Τα θέματα ασφάλειας δεδομένων που προκύπτουν αντιμετωπίζονται και αξιολογούνται σε σταθερή βάση για όλα τα έργα.

γ. Όλα τα έργα που άπτονται της δράσης της Εθνικής Αρχής Στοιχημάτων υποβάλλονται σε περιοδικούς ελέγχους ασφάλειας.

ΜΕΡΟΣ 5 – ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΕΓΚΑΤΑΣΤΑΣΕΩΝ

5.1 Η πρόσβαση επιτρέπεται αναλόγως εξουσιοδότησης και εργασίας. Συνεπώς, οι Εξωτερικοί Χρήστες πρέπει να φέρουν ανά πάσα στιγμή την κάρτα πρόσβασης που τους παρέχει η Αρχή. Σε καμία περίπτωση δεν επιτρέπεται ο Εξωτερικός Χρήστης να δανείσει την κάρτα πρόσβασής του σε κάποιο άλλο άτομο. Η πλαστοπροσωπία είναι παράνομη και απαγορεύεται αυστηρά.

5.2 Τα εργαλεία πρόσβασης (π.χ. κλειδιά, κάρτες πρόσβασης, κλπ.) επιστρέφονται άμεσα με τη διακοπή της σύμβασης εργασίας ή της απασχόλησης του Εξωτερικού Χρήστη.

5.3 Εάν ένα εργαλείο πρόσβασης, όπως κλειδί ή κάρτα πρόσβασης χαθεί πρέπει να αναφερθεί άμεσα στην Αρχή.

5.4 Οι επισκέπτες πρέπει να ταυτοποιούνται και εγκρίνονται πριν από την είσοδο τους στις Εγκαταστάσεις της Αρχής και πρέπει να συνοδεύονται και/ή να φέρουν κάρτα επισκέπτη.

ΜΕΡΟΣ 6 – ΑΝΤΙΙΙΚΗ ΠΡΟΣΤΑΣΙΑ ΛΟΓΙΣΜΙΚΟΥ

6.1 Τα συστήματα που επηρεάζονται συνήθως από ιούς (συμπεριλαμβανομένων των ηλεκτρονικών υπολογιστών και των διακομιστών) πρέπει να προστατεύονται με κατάλληλα αντιιικά προγράμματα (antivirus), προγράμματα προστασίας (firewall), και άλλα λογισμικά ασφάλειας διαδικτύου. Τα λογισμικά και τα προγράμματα ασφαλείας ανανεώνονται σύμφωνα με τις τελευταίες εκδόσεις και αναβαθμίσεις τους.

6.2 Τα Συστήματα ΤΠ που προστατεύονται από αντιιικά λογισμικά πρέπει να υπόκεινται σε ολοκληρωμένους ελέγχους συστήματος τουλάχιστο μια φορά την εβδομάδα. Η βιβλιοθήκη αναγνώρισης ιών (virus definitions library) πρέπει να ανανεώνεται καθημερινά.

ΜΕΡΟΣ 7 – ΠΟΛΙΤΙΚΗ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ

7.1 Οι κινητές συσκευές (συμπεριλαμβανομένων φορητών υπολογιστών, tablet και smartphone) που παρέχονται από την Αρχή πρέπει να μεταφέρονται πάντα με ασφάλεια και να τυγχάνουν προσεκτικού χειρισμού. Οι Εξωτερικοί Χρήστες πρέπει να αποφεύγουν να αφήνουν τις κινητές αυτές συσκευές αφύλακτες σε οιονδήποτε μέρος πέραν της οικίας τους ή των εγκαταστάσεων της Αρχής. Εάν πρέπει να αφήσουν τη συσκευή στο αμάξι, πρέπει να την τοποθετήσουν σε χώρο μη ορατό, εάν είναι δυνατό σε χώρο που κλειδώνει.

7.2 Οι κινητές συσκευές (συμπεριλαμβανομένων φορητών υπολογιστών, tablet και smartphone) προστατεύονται με επιπρόσθετα μέτρα ασφάλειας, όπως κωδικό πρόσβασης οιασδήποτε μορφής.

7.3 Οι κινητές συσκευές (συμπεριλαμβανομένων φορητών υπολογιστών, tablet και smartphone) που παρέχονται από την Αρχή κλειδώνουν, τίθενται σε λειτουργία αναμονής (sleep mode) ή σε άλλη μορφή, μετά από περίοδο αδράνειας, όπως αυτή καθορίζεται από την Αρχή και απαιτείται κωδικός ασφάλειας για την επαναλειτουργία τους. Οι Εξωτερικοί Χρήστες δεν δύναται να αλλάξουν την περίοδο αδράνειας.

ΜΕΡΟΣ 8 – ΠΟΛΙΤΙΚΗ ΚΩΔΙΚΟΥ ΠΡΟΣΒΑΣΗΣ

8.1 Οι κωδικοί πρόσβασης, όπου το επιτρέπει το λογισμικό, ο υπολογιστής ή η συσκευή, πρέπει να:

α. περιέχουν τουλάχιστο οκτώ ψηφία,
β. περιέχουν συνδυασμό κεφαλαίων και μικρών γραμμάτων, αριθμών και συμβόλων,
γ. επαναρρυθμίζονται κάθε τρεις μήνες το αργότερο,
δ. διαφέρουν από τους τελευταίους δώδεκα κωδικούς πρόσβασης Εξωτερικού Χρήστη,
ε. μην είναι προφανείς ή να μαντεύονται εύκολα (π.χ. ημερομηνίες γέννησης ή άλλες ημερομηνίες, ονόματα, σημαντικά γεγονότα, μέρη, κλπ.).

8.2 Οι κωδικοί πρόσβασης θεωρούνται ευαίσθητη και απόρρητη πληροφορία. Συνεπώς, οι Εξωτερικοί Χρήστες δεν πρέπει να μοιράζονται τους κωδικούς πρόσβασής τους με κανένα άλλο πρόσωπο εντός ή εκτός της Αρχής, συμπεριλαμβανομένων των υπεύθυνων Τμημάτων, συναδέλφων συγγενών κλπ.

8.3 Οι κωδικοί πρόσβασης δεν πρέπει σε καμία περίπτωση να αποστέλλονται με email, εφαρμογές γραπτής επικοινωνίας ή οιονδήποτε άλλο τρόπο.

8.4 Στην περίπτωση που οι κωδικοί πρόσβασης χρειάζεται να αποθηκευτούν, αυτό πρέπει να γίνεται με ασφάλεια, με τη χρήση κατάλληλου λογισμικού Οι κωδικοί πρόσβασης δεν πρέπει σε καμία περίπτωση να καταγράφονται σε χαρτί ή να αφήνονται εκτεθειμένοι.

8.5 Εάν ένας Εξωτερικός Χρήστης ξεχάσει τον κωδικό πρόσβασής του, αυτό πρέπει να αναφερθεί στην Αρχή έτσι ώστε να προβεί στα κατάλληλα βήματα για να ανακτήσει ο Εξωτερικός Χρήστης πρόσβαση στα Συστήματα της Αρχής.

8.6 Οι κωδικοί πρόσβασης που χρησιμοποιούνται για εταιρική πρόσβαση δεν μπορούν να χρησιμοποιούνται για κανένα άλλο σκοπό, όπως πρόσβαση σε προσωπικούς λογαριασμούς ηλεκτρονικής αλληλογραφίας, προσωπικές ηλεκτρονικές τραπεζικές συναλλαγές, κλπ.

8.7 Σε περιπτώσεις ενδείξεων ότι, διακυβεύεται η μυστικότητα/ασφάλεια ενός κωδικού ή άλλου παρόμοιου στοιχείου που χρησιμοποιείται για την επιβεβαίωση της ταυτότητας του χρήστη, επιβάλλεται η αλλαγή του κωδικού ή/και του παρόμοιου στοιχείου από το χρήστη. Σε τέτοια περίπτωση, η αλλαγή δύναται να γίνεται μονομερώς από το Τμήμα ΤΠ.

ΜΕΡΟΣ 9 – ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΡΟΣΒΑΣΗΣ ΕΞ ΑΠΟΣΤΑΣΕΩΣ

9.1 Η εξ αποστάσεως πρόσβαση στα εσωτερικά δίκτυα της Αρχής μπορεί να επιτραπεί σε Εξωτερικούς Χρήστες υπό τις ακόλουθες αυστηρές προϋποθέσεις:

α. Οι Εξωτερικοί Χρήστες πρέπει να λάβουν εξουσιοδότηση από την Αρχή που να τους επιτρέπει να έχουν εξ αποστάσεως πρόσβαση στα συστήματα της Αρχής.
β. Η πρόσβαση πρέπει να είναι ασφαλής, με την εφαρμογή του κατάλληλου πρωτοκόλλου κρυπτογράφησης (όπως Εικονικό Προσωπικό Δίκτυο) και δυνατών κωδικών φράσεων. Οι κωδικοί πρόσβασης πρέπει να πληρούν τους όρους που παρατίθενται στην *Πολιτική Κωδικού Πρόσβασης* (Μέρος 8),
γ. Η εξ αποστάσεως σύνδεση πρέπει να πραγματοποιείται μέσω συσκευής δέκτη που να προστατεύεται πρόσφατη έκδοση αντιικού λογισμικού καθώς και με πρόσφατη έκδοση όλων των εφαρμογών και λειτουργικού συστήματος (συμπεριλαμβανομένων των προγραμμάτων ασφάλειας),
δ. Οι εξουσιοδοτημένοι Εξωτερικοί Χρήστες πρέπει να πραγματοποιούν εξ αποστάσεως πρόσβαση μόνο εάν βρίσκονται συνδεδεμένοι στο δίκτυο της οικίας τους ή σε ασφαλές δίκτυο τρίτου το οποίο εμπιστεύονται. Η σύνδεση μέσα από μη ασφαλή, δημόσια δίκτυα (π.χ. καφέ, εστιατόρια, αεροδρόμια, κλπ.) πρέπει να αποφεύγεται.

9.2 Η Αρχή διατηρεί το δικαίωμα να ανακαλέσει μονομερώς, να αναστείλει ή να ακυρώσει την πρόσβαση εξ αποστάσεως ενός Εξωτερικού Χρήστη ανά πάσα στιγμή.

ΜΕΡΟΣ 10 – ΠΟΛΙΤΙΚΗ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ ΔΕΔΟΜΕΝΩΝ

10.1 Τα δεδομένα που κατέχει η Αρχή κατηγοριοποιούνται σε μια από τις πιο κάτω κατηγορίες:

- **Αυστηρώς/άκρως εμπιστευτικά**

Ορισμός: Δεδομένα σε οποιαδήποτε μορφή που έχουν συλλεγεί, κατέχονται και τυγχάνουν επεξεργασίας από ή για λογαριασμό της Αρχής και υπόκεινται σε συγκεκριμένη προστασία σύμφωνα με τις εθνικές ή ευρωπαϊκές νομοθεσίες, κανονισμούς ή ισχύουσες συμβάσεις.

Παραδείγματα: Αρχεία που περιέχουν προσωπικά δεδομένα ατόμων, όπως καταστάσεις προσωπικού, αρχεία που αφορούν το προσωπικό των εποπτευόμενων νομικών προσώπων, αρχεία που αφορούν εποπτευόμενα φυσικά πρόσωπα, συμφωνίες με εξωτερικούς συνεργάτες, στοιχηματική δραστηριότητα ατόμων, κλπ.

- **Εμπιστευτικά**

Ορισμός: Δεδομένα των οποίων η απώλεια, τροποποίηση ή μη εξουσιοδοτημένη δημοσιοποίηση θα μπορούσε να προκαλέσει βλάβη στη λειτουργία της Αρχής, οικονομική απώλεια, πλήγμα στη φήμη της Αρχής ή νομικές ευθύνες.

Παραδείγματα: Εσωτερικές εκθέσεις, Πολιτικές και Διαδικασίες ΕΑΣ, τηλεφωνικό αρχείο ΕΑΣ, κλπ.

- **Αποκλειστικά Για Εσωτερική Χρήση**

Ορισμός: Δεδομένα των οποίων η μη εξουσιοδοτημένη δημοσιοποίηση, τροποποίηση ή καταστροφή δεν αναμένεται να έχει σοβαρές ή αρνητικές συνέπειες στην Αρχή, στο προσωπικό, σε εξωτερικούς συνεργάτες ή εποπτευόμενα μέρη.

Παραδείγματα: Υλικό εκπαίδευσης, Εγχειρίδια, κλπ.

- **Άδειες**

Ορίζονται αποκλειστικά για άδειες παροχής υπηρεσιών στοιχήματος τις οποίες εκδίδει η Αρχή.

Παραδείγματα: Άδεια αποδέκτη Κλάσης Α, άδεια αποδέκτη Κλάσης Β, άδεια εξουσιοδοτημένου αντιπροσώπου αποδέκτη Κλάσης Α, άδεια υποστατικού και επιστολές υπεύθυνων προσώπων.

- **Δημόσια**

Ορισμός: Δεδομένα που δεν υπόκεινται σε καμία από τις άλλες τρεις κατηγορίες και μπορούν να δημοσιοποιηθούν χωρίς να απαιτείται συγκεκριμένη έγκριση.

Παραδείγματα: Δημόσιες ανακοινώσεις, Κατάλογος αδειούχων εποπτευομένων (αποδέκτες, εξουσιοδοτημένοι αντιπρόσωποι, υποστατικά), Λίστα αποκλεισμού, Στρατηγικός σχεδιασμός, κλπ.

ΜΕΡΟΣ 11 – ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Εμπιστευτικά Δεδομένα

11.1 Σε περίπτωση που χρειάζεται να μεταφερθούν εμπιστευτικά δεδομένα σε ηλεκτρονικά μέσα ή συσκευές, πρέπει να κρυπτογραφούνται, εκτός και εάν η εμπιστευτικότητά τους διασφαλίζεται με άλλο τρόπο.

11.2 Τα εμπιστευτικά δεδομένα που μεταφέρονται από ένα σημείο σε άλλο πρέπει να μεταφέρονται σε κατάλληλο φάκελο/μέσο μεταφοράς όπου να αναγράφεται η λέξη «εμπιστευτικό». Η μεταφορά πρέπει να γίνεται με ασφαλή υπηρεσία μεταφοράς ή άλλο εγκεκριμένο τρόπο μεταφοράς που μπορεί να εντοπιστεί με ακρίβεια.

Εμπιστευτικά ή Άκρως Εμπιστευτικά Δεδομένα

11.3 Τα εμπιστευτικά ή άκρως εμπιστευτικά δεδομένα που αποθηκεύονται ηλεκτρονικά στα Συστήματα ΤΠ της Αρχής, πρέπει να αποθηκεύονται με ασφάλεια, εφαρμόζοντας ελεγχόμενη πρόσβαση.

11.4 Τα έντυπα αρχεία που περιέχουν εμπιστευτικά ή άκρως εμπιστευτικά δεδομένα όπως αυτά καθορίζονται στην *Πολιτική Εμπιστευτικότητας Δεδομένων* (Μέρος 10) φυλάγονται σε κλειδωμένα ντουλάπια σε χώρους με ελεγχόμενη πρόσβαση στις εγκαταστάσεις της Αρχής.

11.5 Στις περιπτώσεις που τα εμπιστευτικά ή άκρως εμπιστευτικά δεδομένα χρειάζεται να μεταφερθούν μέσα από τα δίκτυα, η εμπιστευτικότητά τους διασφαλίζεται με κατάλληλες τεχνικές κρυπτογράφησης.

11.6 Η εκτύπωση ή φωτοτύπηση αρχείων με εμπιστευτικά ή άκρως εμπιστευτικά δεδομένα αποφεύγεται όπου είναι δυνατόν και επιτρέπεται μόνο σε εκτυπωτές και φωτοτυπικές μηχανές της Αρχής, οι οποίες είναι συνδεδεμένες με το εσωτερικό δίκτυο και προστατεύονται συνεπώς με τον κατάλληλο εξοπλισμό δικτύου (firewall).

Αυστηρώς/άκρως Εμπιστευτικά Δεδομένα

11.7 Τα αυστηρώς εμπιστευτικά δεδομένα απαγορεύεται να αποθηκεύονται ή να μεταφέρονται σε οιανδήποτε κινητή συσκευή (συμπεριλαμβανομένων των φορητών υπολογιστών, tablet και smartphone) ή σε άλλο μέσο (συμπεριλαμβανομένων USB stick ή δίσκους οποιουδήποτε είδους), είτε αυτά ανήκουν στην Αρχή ή όχι.

11.8 Η φυσική μεταφορά έντυπων εγγράφων που περιέχουν άκρως εμπιστευτικά δεδομένα πρέπει να αποφεύγεται όπου είναι δυνατόν. Στις περιπτώσεις που η φυσική μεταφορά είναι απαραίτητη, τα αρχεία αυτά πρέπει να μεταφέρονται σε φάκελο/μέσο στο οποίο να αναγράφεται «Άκρως Εμπιστευτικό» υπό την επίβλεψη εξουσιοδοτημένου λειτουργού της Αρχής.

11.9 Οι Εξωτερικοί Χρήστες που χειρίζονται αυστηρώς εμπιστευτικά δεδομένα εκ μέρους της Αρχής υπόκεινται και οφείλουν να συμμορφώνονται με τους ακόλουθους όρους:

α. Τα emails που περιέχουν άκρως εμπιστευτικά δεδομένα πρέπει να κρυπτογραφούνται και να επισημαίνονται ως «άκρως εμπιστευτικά»,
β. Τα άκρως εμπιστευτικά δεδομένα μπορούν να μεταφέρονται μόνο μέσα από ασφαλή δίκτυα. Η μεταφορά τους από μη ασφαλή δίκτυα δεν επιτρέπεται σε καμία περίπτωση,
γ. Τα άκρως εμπιστευτικά δεδομένα που περιέχονται στο κείμενο ενός email, είτε αποστέλλονται είτε λαμβάνονται, πρέπει να αποθηκεύονται με ασφάλεια.

11.10 Τα προσωπικά δεδομένα (όπως αυτά καθορίζονται στο ΓΚΠΔ) που συλλέγονται, φυλάγονται και τυγχάνουν επεξεργασίας από την Αρχή, τυγχάνουν διαχείρισης σύμφωνα με τις αρχές και τις οδηγίες του ΓΚΠΔ.

11.11 Η Αρχή διασφαλίζει ότι τα προσωπικά δεδομένα που συλλέγονται, αποθηκεύονται μόνο για όσο διάστημα κρίνεται απαραίτητο για να τον σκοπό της συλλογής τους.

11.12 Σε περίπτωση που τυχόν παραβίαση της ασφάλειας προκαλέσει ακούσια ή παράνομη καταστροφή, απώλεια, αλλοίωση, παράτυπη δημοσιοποίηση ή πρόσβαση σε προσωπικά

δεδομένα, ο Λειτουργός Προστασίας Δεδομένων της Αρχής καλείται άμεσα ούτως ώστε να προβεί σε άμεση αξιολόγηση του ρίσκου των δικαιωμάτων και ελευθεριών των ατόμων και εάν κριθεί κατάλληλο, αναφέρει την εν λόγω παραβίαση στη σχετική Αρχή Προστασίας Δεδομένων.

Μεταφορά πληροφοριών

11.13 Καθορίζονται συμφωνίες, όπως επίσημες συμβάσεις και συμβάσεις λογισμικών, σε σχέση με τη μεταφορά και ανταλλαγή πληροφοριών και λογισμικών μεταξύ οργανισμών, οι οποίες είναι συμβατές με τη σχετική νομοθεσία. Οι διαδικασίες εφαρμόζονται σε κάθε τομέα όπου λαμβάνονται ή από τον οποίο αποστέλλονται πληροφορίες, για να διασφαλίζεται η ασφάλεια μεταφοράς και ανταλλαγής πληροφοριών σύμφωνα με τις πρόνοιες της πολιτικής της Εθνικής Αρχής Στοιχημάτων.

ΜΕΡΟΣ 12 – ΑΝΑΦΟΡΑ ΠΑΡΑΒΙΑΣΕΩΝ ΑΣΦΑΛΕΙΑΣ

12.1 Οι ανησυχίες, απορίες, υποψίες ή πληροφορίες για τυχόν παραβιάσεις πρέπει να αναφέρονται στην Αρχή μέσω τηλεφώνου στο 22881800 ή υποβολής σχετικής αναφοράς από την ιστοσελίδα της Αρχής https://nba.gov.cy/en/incident-reporting-form/. Οι αναφορές περιστατικών που σχετίζονται με την ασφάλεια πρέπει να φτάνουν στα κατάλληλα άτομα της διοίκησης της Αρχής χωρίς καθυστέρηση.

12.2 Οι ανησυχίες, απορίες, υποψίες ή πληροφορίες για τυχόν παραβιάσεις που σχετίζονται με προσωπικά δεδομένα πρέπει να αναφέρονται άμεσα στην Αρχή και τον Λειτουργό Προστασίας Δεδομένων της Αρχής μέσω του ηλεκτρονικού ταχυδρομείου dpo@nba.gov.cy ή τηλεφωνικά στο 22881800, ο οποίος πρέπει να χειριστεί το θέμα στο πλαίσιο της Πολιτικής Προστασίας Δεδομένων της Αρχής.

12.3 Αμέσως μετά τη λήψη ερωτήματος ή αναφοράς για παραβίαση, το Τμήμα ΤΠ πρέπει σε εύλογο χρονικό διάστημα να αξιολογήσει την κατάσταση και το επίπεδο κινδύνου και να προβεί στις ενέργειες που κρίνει απαραίτητες για να αντιμετωπίσει το ζήτημα. Εάν υπάρχει υποψία εγκληματικής πράξης, πρέπει να ειδοποιηθούν οι αστυνομικές αρχές.

12.4 Σε καμία περίπτωση δεν επιτρέπεται ένας Εξωτερικός Χρήστης να επιχειρήσει να επιλύσει θέμα παραβίασης ασφάλειας από μόνος του, χωρίς πρώτα να ενημερώσει την Αρχή.

ΜΕΡΟΣ 13 – ΠΟΛΙΤΙΚΗ ΧΡΗΣΗΣ ΔΙΑΔΙΚΤΥΟΥ ΕΝΤΟΣ ΤΩΝ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΤΗΣ ΑΡΧΗΣ

13.1 Οι Εξωτερικοί Χρήστες θα πρέπει να χρησιμοποιούν το διαδίκτυο με τρόπο υπεύθυνο και επαγγελματικό που να συνάδει με την εκτέλεση των απαιτούμενων εργασιών.

13.2 Η Αρχή παρέχει στους Εξωτερικούς Χρήστες πρόσβαση στο διαδίκτυο με μοναδικό στόχο τη διευκόλυνση της εκτέλεσης των εκάστοτε εργασιών τους.

13.3 Η μεταφορά μεγάλου όγκου δεδομένων από το διαδίκτυο πρέπει να αποφεύγεται κατά τη χρήση του διαδικτύου της Αρχής.

13.4 Οι Εξωτερικοί Χρήστες δεν επιτρέπεται σε καμία περίπτωση να χρησιμοποιούν το διαδίκτυο για να αποκτήσουν ή να επιχειρήσουν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε αρχεία ή σημεία περιορισμένης πρόσβασης στο δίκτυο της Αρχής.

13.5 Οι Εξωτερικοί Χρήστες δεν επιτρέπεται να κατεβάσουν, να δουν ή να ανακτήσουν υλικό παράνομου, πορνογραφικού, σεξιστικού, ρατσιστικού, προσβλητικού ή ανήθικου περιεχομένου. Απαγορεύεται αυστηρά η πρόσβαση σε υλικό που μπορεί να θεωρηθεί προσβλητικό για κάποιο άτομο ή που μπορεί να φέρει την Αρχή σε δύσκολη θέση ή να βλάψει τη φήμη και την εικόνα της.

13.6 Ο εξοπλισμός δικτύου της αρχής δεν επιτρέπει σε συγκεκριμένες συσκευές πρόσβαση σε ορισμένες ιστοσελίδες. Εάν υπάρχει σοβαρή ανάγκη σύνδεσης του Εξωτερικού Χρήστη με μια αποκλεισμένη ιστοσελίδα για επαγγελματικό σκοπό, χρειάζεται να λάβει έγκριση από την Αρχή.

13.7 Οι Εξωτερικοί Χρήστες χρειάζεται να έχουν επίγνωση των διαφόρων βαθμών εμπιστευτικότητας των δεδομένων όπως καθορίζονται από την Αρχή, και να διασφαλίζουν ότι εμπιστευτικά ή αυστηρώς εμπιστευτικά δεδομένα δεν διαχέονται ποτέ σε ηλεκτρονική επικοινωνία.

ΜΕΡΟΣ 14 –ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΡΟΜΗΘΕΥΤΩΝ/ΠΩΛΗΤΩΝ

14.1 Οι συμβαλλόμενοι Προμηθευτές και Πωλητές δηλώνουν ότι έχουν μελετήσει και κατανοούν την παρούσα Πολιτική και όλες τις άλλες Πολιτικές που σχετίζονται με την υπηρεσία που προσφέρουν.

14.2 Οι Εξωτερικοί Χρήστες δηλώνουν ότι έχουν διαβάσει και μελετήσει την παρούσα Πολιτική και όλες τις άλλες Πολιτικές που σχετίζονται με την υπηρεσία που προσφέρουν.

ΜΕΡΟΣ 15 – ΑΠΟΔΕΚΤΗ ΧΡΗΣΗ ΕΞΟΠΛΙΣΜΟΥ

α. Οι Εξωτερικοί Χρήστες έχουν εξουσιοδότηση να χρησιμοποιούν τις πληροφορίες της ΕΑΣ μόνο για σκοπούς που σχετίζονται με την εκτέλεση των εκάστοτε εργασιών τους για τους οποίους τους έχει δοθεί εξουσιοδότηση.
β. Οι Εξωτερικοί Χρήστες οφείλουν να διακόπτουν τις ενεργές κλήσεις ή συνεδριάσεις με την Αρχή όταν αυτές ολοκληρώνονται.
γ. Οι Εξωτερικοί Χρήστες απαγορεύεται να μετατρέπουν τις ρυθμίσεις, να αφαιρούν, να απενεργοποιούν, να αλλάζουν ή να παρακάμπτουν ελέγχους ασφαλείας όπως λογισμικά προστασίας από ιούς, να μεταβάλλουν καταχωρήσεις ή καταγραφή λειτουργίας στις συσκευές ή/και εξοπλισμό της Αρχής που χρησιμοποιούνται από αυτούς.
δ. Η εγκατάσταση ή αφαίρεση ενός λογισμικού από τον εξοπλισμό της Αρχής πραγματοποιείται μόνο υπό την ευθύνη εξουσιοδοτημένων μελών του Τμήματος ΤΠ της Αρχής.

ε. Οι Εξωτερικοί Χρήστες οφείλουν να ανοίγουν/κατεβάζουν αρχεία από το διαδίκτυο μόνο από νόμιμους, αξιόπιστους αποστολείς/πηγές, και αφού σιγουρευτούν ότι το αντιιικό πρόγραμμα έχει ελέγξει τα εν λόγω αρχεία.

στ. Σε περίπτωση αμφιβολίας, δεν πρέπει να ανοίγονται, να κατεβάζονται ή να τρέχουν ύποπτα αρχεία ή συνημμένα.

ΜΕΡΟΣ 16 – ΛΕΙΤΟΥΡΓΙΚΕΣ ΔΙΑΔΙΚΑΣΙΕΣ ΚΑΙ ΚΑΘΗΚΟΝΤΑ

16.1 Απαιτήσεις από εξωτερικούς συνεργάτες

α. Οι απαιτήσεις ανάπτυξης που απορρέουν από αυτήν την πολιτική ισχύουν εξίσου για προϊόντα που αγοράζονται από την αγορά ή που αναπτύσσονται κατά παραγγελία για την ΕΑΣ. Επιπρόσθετα, χρειάζεται να τηρούνται οι ακόλουθες προϋποθέσεις:

- Τα συμβόλαια με τρίτους δεν περιορίζονται στις απαιτήσεις του προϊόντος ή της υπηρεσίας αλλά επίσης περιλαμβάνουν όρους που σχετίζονται με τη διασφάλιση της ασφάλειας. Λογισμικά που προσφέρουν αυξημένη λειτουργικότητα εις βάρος των ελέγχων ασφαλείας απορρίπτονται.
- Τα συστήματα που αναπτύσσονται από τρίτους για τις ανάγκες του Οργανισμού υπόκεινται σε ενδελεχή έλεγχο για την εξασφάλιση τόσο της ποιότητας όσο και της ακρίβειας της εργασίας, καθώς επίσης και για τον εντοπισμό πιθανώς κακόβουλου κώδικα πριν την εφαρμογή τους.

β. Η ανάπτυξη λογισμικού από τρίτους επιβλέπεται και ελέγχεται από το Τμήμα ΤΠ της Αρχής, λαμβάνοντας υπόψιν τα πιο κάτω θέματα:

- Διαχείριση αδειών, δικαιώματα πνευματικής ιδιοκτησίας και ιδιοκτησία κώδικα,
- Έλεγχος διαδικασιών ποιότητας και ανάπτυξης συστημάτων,
- Δικαίωμα πρόσβασης για έλεγχο ποιότητας και ακρίβειας.

ΜΕΡΟΣ 17 – ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΗΣ

Η παρούσα Πολιτική αναθεωρείται σε ετήσια βάση και ανανεώνεται όπως χρειάζεται για να προσαρμόζεται στις αλλαγές των λειτουργικών σκοπών και/ή στο πλαίσιο επικινδυνότητας. Οι αναθεωρημένες εκδόσεις της Πολιτικής θα αποστέλλονται σε όλους τους Εξωτερικούς Χρήστες και όλα τα εμπλεκόμενα μέρη προς ενημέρωση τους. Απορίες, ερωτήματα, ανησυχίες και κάθε μορφή ανατροφοδότησης σε σχέση με την Πολιτική πρέπει να αποστέλλεται στον Λειτουργό Συμμόρφωσης, complianceofficer@nba.gov.cy και/ή στον Λειτουργό Προστασίας Δεδομένων, dpo@nba.gov.cy, της Αρχής.

ΜΕΡΟΣ 18 – ΕΦΑΡΜΟΓΗ ΠΟΛΙΤΙΚΗΣ

Η παρούσα Πολιτική τίθεται σε πλήρη εφαρμογή τον Μάρτιο του 2023. Κανένα μέρος της Πολιτικής δεν θα έχει αναδρομική ισχύ, αλλά θα εφαρμόζεται μόνο για θέματα που προκύπτουν από αυτή την ημερομηνία και έπειτα. Κάθε εκούσια ή ακούσια παραβίαση της

παρούσας Πολιτικής από τους Εξωτερικούς Χρήστες θα τυγχάνει κατάλληλου χειρισμού από την Αρχή.