					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P08					Τίτλος εγγράφου: **Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 01.01.2025			Ιδιοκτήτης εγγράφου:							
X	Πολιτική		Πρότυπο		Διαδικασία		Έντυπο		Μητρώο		Άλλο	

Ιστορικό αναθεωρήσεων				
Αριθμός αναθεώρησης	**Ημερομηνία αναθεώρησης**	**Αλλαγές**	**Ελέγχθηκε από**	**Ιδιοκτήτης διεργασίας**

Εγκρίσεις			
Όνομα	**Θέση**	**Ημερομηνία**	**Υπογραφή**

Ευθυγράμμιση με πρότυπα και κανονισμούς

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρα 7.3, Παράρτημα Α Έλεγχος 6.3	Καθορίζει απαιτήσεις ευαισθητοποίησης και εκπαίδευσης που καλύπτονται από την παρούσα πολιτική
ISO/IEC 27002:2022	Έλεγχος 6	Υποστηρίζει κατάλληλη εκπαίδευση βάσει ρόλων, ανάλογα με τον εργασιακό ρόλο
NIST SP 800-53 Rev.5	AT-1 έως AT-5	Ευθυγραμμίζεται με την πολιτική και τις διαδικασίες, την εκπαίδευση ευαισθητοποίησης, την εκπαίδευση βάσει ρόλων, τα αρχεία εκπαίδευσης και την επικοινωνία με τις ομάδες ασφάλειας
ΓΚΠΔ της ΕΕ	Άρθρα 32, 39· Αιτιολογική σκέψη 78	Επιβάλλει εκπαίδευση για όσους χειρίζονται δεδομένα προσωπικού χαρακτήρα και γενική ευαισθητοποίηση του προσωπικού
Οδηγία NIS2 της ΕΕ	Άρθρα 21(2)(a, b), 21(3)	Απαιτεί πολιτικές εκπαίδευσης για κινδύνους και ασφάλεια, καθώς και πρωτοβουλίες ευαισθητοποίησης
Κανονισμός DORA της ΕΕ	Άρθρα 5, 8, 13	Απαιτεί ευαισθητοποίηση και εκπαίδευση σχετικά με τον κίνδυνο ΤΠΕ ως μέρος των ελέγχων ανθεκτικότητας
COBIT 2019	APO07, DSS05, MEA	Ενισχύει την ευαισθητοποίηση του ανθρώπινου δυναμικού, την εκπαίδευση χρηστών και την παρακολούθηση της συμμόρφωσης

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει το επίσημο πλαίσιο για τη διασφάλιση ότι όλο το προσωπικό ενημερώνεται για τις αρμοδιότητές του ως προς την ασφάλεια πληροφοριών και λαμβάνει την απαιτούμενη εκπαίδευση για την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών περιουσιακών στοιχείων.

1.2 Υποστηρίζει τη Ρήτρα 7.3 του ISO/IEC 27001 και τον Έλεγχο 6.3 του Παραρτήματος Α, απαιτώντας ένα δομημένο, βασισμένο στον κίνδυνο πρόγραμμα ευαισθητοποίησης και εκπαίδευσης, προσαρμοσμένο στους οργανωτικούς ρόλους και στο εξελισσόμενο τοπίο απειλών.

1.3 Η πολιτική συμβάλλει στη μείωση ευπαθειών που σχετίζονται με τον ανθρώπινο παράγοντα, στην προώθηση συμπεριφοράς με επίγνωση θεμάτων ασφάλειας και στη συνεχή ενίσχυση ασφαλών πρακτικών, σύμφωνα με τις κανονιστικές και συμβατικές απαιτήσεις.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα εσωτερικά και εξωτερικά φυσικά πρόσωπα που έχουν πρόσβαση σε πληροφοριακά συστήματα, δεδομένα ή εγκαταστάσεις του οργανισμού, συμπεριλαμβανομένων των εξής:

2.1.1 Εργαζομένων (πλήρους απασχόλησης, μερικής απασχόλησης, προσωρινών)

2.1.2 Εργολάβων και παρόχων υπηρεσιών τρίτων μερών, συμβούλων, προμηθευτών και ασκουμένων

2.1.3 Τρίτων μερών με λογική ή φυσική πρόσβαση βάσει συμφωνιών παροχής υπηρεσιών

2.2 Το πεδίο εφαρμογής περιλαμβάνει:

2.2.1 Αρχική εκπαίδευση ευαισθητοποίησης για την ασφάλεια κατά την ένταξη

2.2.2 Εκπαίδευση ειδική ανά ρόλο (π.χ. προγραμματιστές, οικονομικές υπηρεσίες, χρήστες υψηλών δικαιωμάτων)

2.2.3 Περιοδική επανεκπαίδευση και εκστρατείες ευαισθητοποίησης

2.2.4 Έκτακτη εκπαίδευση σε απόκριση σε περιστατικά ή νέες απειλές

2.3 Οι μέθοδοι παροχής εκπαίδευσης που καλύπτονται από την παρούσα πολιτική περιλαμβάνουν ηλεκτρονική μάθηση, δια ζώσης ενημερώσεις, προσομοιώσεις, δοκιμασίες γνώσεων, αφίσες, ενημερωτικά δελτία και υποχρεωτικές επιβεβαιώσεις.

3. Στόχοι

3.1 Να διασφαλίζεται ότι όλο το προσωπικό κατανοεί τις αρμοδιότητές του για την προστασία των περιουσιακών στοιχείων του οργανισμού και για τη συμμόρφωση με τις πολιτικές ασφάλειας.

3.2 Να παρέχεται συνεχής και μετρήσιμη εκπαίδευση ευαισθητοποίησης για την ασφάλεια, ευθυγραμμισμένη με την έκθεση σε κίνδυνο ανά ρόλο.

3.3 Να ενσωματώνονται ασφαλείς συμπεριφορές στην καθημερινή λειτουργία μέσω της ενίσχυσης πρακτικών όπως η ασφαλής χρήση κωδικών πρόσβασης, η αναφορά περιστατικών και η ανθεκτικότητα στο phishing.

3.4 Να διασφαλίζεται η συμμόρφωση με κανονιστικές απαιτήσεις και η ετοιμότητα για έλεγχο ως προς τις υποχρεώσεις εκπαίδευσης ασφάλειας πληροφοριών σε όλους τους κλάδους και τις δικαιοδοσίες.

3.5 Να μειώνονται τα περιστατικά ασφάλειας που προκύπτουν από αμέλεια, έλλειψη ενημέρωσης ή εσφαλμένη κρίση μέσω διαμόρφωσης συμπεριφοράς και συνεχούς ενίσχυσης.

4. Ρόλοι και αρμοδιότητες

4.1 Εκτελεστική Διοίκηση

4.1.1 Εγκρίνει τη στρατηγική εκπαίδευσης στην ασφάλεια πληροφοριών του οργανισμού και διασφαλίζει ότι διατίθενται οι αναγκαίοι πόροι και ότι αυτή ενσωματώνεται στις εταιρικές προτεραιότητες.

4.1.2 Παρακολουθεί τη συμμόρφωση σε επίπεδο διοίκησης και διασφαλίζει την τήρηση της πολιτικής σε όλα τα τμήματα.

4.2 Επικεφαλής Ασφάλειας Πληροφοριών / Υπεύθυνος ΣΔΑΠ

4.2.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και καθορίζει το πλαίσιο ευαισθητοποίησης και εκπαίδευσης σύμφωνα με τις ανάγκες κινδύνου, συμμόρφωσης και επιχειρησιακής λειτουργίας.

4.2.2 Ασκεί εποπτεία στον σχεδιασμό, την παροχή, την παρακολούθηση, την ιχνηλάτηση και την ανασκόπηση όλων των πρωτοβουλιών εκπαίδευσης ασφάλειας.

4.2.3 Διασφαλίζει ότι η εκπαίδευση επικαιροποιείται περιοδικά και αντανακλά τις εξελισσόμενες απειλές και τις αναδυόμενες τεχνολογίες.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Απαιτήσεις ανασκόπησης και επικαιροποίησης

9.1 Συχνότητα ανασκόπησης

9.1.1 Η παρούσα πολιτική και το σχετικό πρόγραμμα εκπαίδευσης πρέπει να ανασκοπούνται:

9.1.1.1 ετησίως, ή

9.1.1.2 μετά από σοβαρά περιστατικά που περιλαμβάνουν ανθρώπινο σφάλμα ή εσωτερική απειλή

9.1.1.3 κατά την εισαγωγή σημαντικών νέων τεχνολογιών ή απειλών

9.1.1.4 σε απόκριση σε αλλαγές νομικών, συμβατικών ή πιστοποιητικών υποχρεώσεων

9.2 Διαδικασία ανασκόπησης

9.2.1 Η ανασκόπηση διενεργείται από τον Επικεφαλής Ασφάλειας Πληροφοριών σε συντονισμό με:

9.2.1.1 τα τμήματα Ανθρώπινου Δυναμικού και Εκπαίδευσης

9.2.1.2 το Νομικό Τμήμα και τους Υπευθύνους Προστασίας Δεδομένων

9.2.1.3 τις λειτουργίες Ασφάλειας Πληροφορικής και Επιχειρησιακού Κινδύνου

9.2.2 Όλες οι επικαιροποιήσεις πρέπει:

9.2.2.1 Να εγκρίνονται από την Επιτροπή Καθοδήγησης του ΣΔΑΠ

9.2.2.2 Να ελέγχονται ως προς την έκδοση και να τεκμηριώνονται στο Μητρώο Εγγράφων του ΣΔΑΠ

9.2.2.3 Να κοινοποιούνται στους χρήστες εφόσον ουσιώδεις αλλαγές επηρεάζουν το πεδίο της εκπαίδευσης ή τις αρμοδιότητες

9.3 Διακυβέρνηση επικαιροποίησης περιεχομένου

9.3.1 Οι εκπαιδευτικές ενότητες και το υλικό ευαισθητοποίησης πρέπει να ανασκοπούνται κάθε 12 μήνες, ώστε να διασφαλίζονται:

9.3.1.1 η συνάφεια με το τοπίο απειλών

9.3.1.2 η κανονιστική ακρίβεια

9.3.1.3 η συμβατότητα μορφότυπου (π.χ. προσβασιμότητα, τοπικοποίηση)

9.3.2 Παρωχημένο ή παραπλανητικό περιεχόμενο πρέπει να αποσύρεται άμεσα και να αντικαθίσταται από εγκεκριμένες εναλλακτικές.

10. Σχετικές πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική υποστηρίζεται από και υποστηρίζει την εφαρμογή των εξής:

10.1.1 P01 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει την ευαισθητοποίηση σε θέματα ασφάλειας ως θεμελιώδη έλεγχο στο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) του οργανισμού.

10.1.2 P03 – Πολιτική Αποδεκτής Χρήσης: Απαιτεί επιβεβαίωση από τους χρήστες κατά την εκπαίδευση και αποσαφηνίζει τις αρμοδιότητες που συνδέονται με την καθημερινή χρήση της τεχνολογίας.

10.1.3 P07 – Πολιτική Ένταξης και Αποχώρησης: Διασφαλίζει ότι η εκπαίδευση ενσωματώνεται κατά την ένταξη και παρακολουθείται σε όλη τη διάρκεια της απασχόλησης.

10.1.4 P06 – Πολιτική Διαχείρισης Κινδύνων: Συνδέει την εκπαίδευση με επίκεντρο τον ανθρώπινο παράγοντα με τη μοντελοποίηση απειλών και τις στρατηγικές μείωσης του υπολειπόμενου κινδύνου.

10.1.5 P33 – Πολιτική Ελέγχου και Παρακολούθησης Συμμόρφωσης: Επικυρώνει ότι οι έλεγχοι ευαισθητοποίησης είναι λειτουργικοί, μετρήσιμοι και αποτελεσματικοί κατά τους ελέγχους.

10.2 Από κοινού, οι πολιτικές αυτές συγκροτούν ένα ολοκληρωμένο πλαίσιο ελέγχου συμπεριφοράς που ενσωματώνει ευαισθητοποίηση, λογοδοσία και ενίσχυση της οργανωτικής κουλτούρας.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 7.3 – Ευαισθητοποίηση: Απαιτεί από τους οργανισμούς να διασφαλίζουν ότι οι εργαζόμενοι γνωρίζουν τις πολιτικές ασφάλειας πληροφοριών και τις αρμοδιότητές τους. Η παρούσα πολιτική θέτει την απαίτηση αυτή σε εφαρμογή μέσω δομημένης διαδικασίας ένταξης, περιοδικής εκπαίδευσης και μετρήσιμης συμμετοχής σε εκστρατείες.

11.1.2 Παράρτημα Α Έλεγχος 6.3 – Ευαισθητοποίηση, εκπαίδευση και κατάρτιση για την ασφάλεια πληροφοριών: Καλύπτεται πλήρως μέσω αρχικών, βάσει ρόλων και συνεχιζόμενων προγραμμάτων εκπαίδευσης, προσαρμοσμένων στα προφίλ κινδύνου των χρηστών.

11.2 ISO/IEC 27002:2022 – Έλεγχος 6

11.2.1 Υποστηρίζει την ανάπτυξη και παροχή εκπαίδευσης ευαισθητοποίησης κατάλληλης για τους εργασιακούς ρόλους, με έμφαση στην ενίσχυση ασφαλούς συμπεριφοράς και στην περιοδική επικαιροποίηση βάσει πληροφόρησης για απειλές και ανατροφοδότησης από ελέγχους.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 έως AT-5 (οικογένεια ελέγχων Ευαισθητοποίησης και Εκπαίδευσης): Η παρούσα πολιτική ευθυγραμμίζεται με τα AT-1 (Πολιτική και Διαδικασίες), AT-2 (Εκπαίδευση Ευαισθητοποίησης), AT-3 (Εκπαίδευση βάσει ρόλων), AT-4 (Αρχεία εκπαίδευσης ασφάλειας) και AT-5 (Επικοινωνία με ομάδες ασφάλειας).

11.3.2 IA-5, AC-2: Ενισχύει την ευθύνη των χρηστών για ασφαλή έλεγχο ταυτότητας και αποδεκτή χρήση, που αποτελούν βασικά αποτελέσματα των προγραμμάτων ευαισθητοποίησης.

11.3.3 IR-1 έως IR-8: Η ετοιμότητα απόκρισης σε περιστατικά ενισχύεται μέσω στοχευμένων εκστρατειών ευαισθητοποίησης και προσομοιώσεων.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Απαιτεί το προσωπικό που χειρίζεται δεδομένα προσωπικού χαρακτήρα να είναι εκπαιδευμένο ώστε να αναγνωρίζει, να προλαμβάνει και να αναφέρει κινδύνους για τα δεδομένα προσωπικού χαρακτήρα. Η παρούσα πολιτική διασφαλίζει ότι οι χειριστές δεδομένων και όλοι οι σχετικοί ρόλοι εκπαιδεύονται αναλόγως.

11.4.2 Άρθρο 39 – Καθήκοντα του Υπευθύνου Προστασίας Δεδομένων: Περιλαμβάνει την ευαισθητοποίηση και την εκπαίδευση του προσωπικού που συμμετέχει σε πράξεις επεξεργασίας.

11.4.3 Αιτιολογική σκέψη 78: Ενθαρρύνει κατάλληλα μέτρα ευαισθητοποίησης για τη διασφάλιση ισχυρών πρακτικών ασφάλειας και τήρησης της πολιτικής.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(a, b): Απαιτεί από τους φορείς να υιοθετούν πολιτικές για την ανάλυση κινδύνων και την εκπαίδευση ασφάλειας για όλο το σχετικό προσωπικό. Η παρούσα πολιτική καλύπτει την απαίτηση αυτή θεσπίζοντας συνεχείς, προσαρμοσμένες στον ρόλο διαδικασίες εκπαίδευσης.

11.5.2 Άρθρο 21(3): Ενθαρρύνει την προώθηση της ευαισθητοποίησης ως προς τους κινδύνους κυβερνοασφάλειας μεταξύ διοίκησης και προσωπικού μέσω πρωτοβουλιών ευαισθητοποίησης και προσομοιώσεων.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 13 – Στρατηγική ψηφιακής επιχειρησιακής ανθεκτικότητας: Απαιτεί η ευαισθητοποίηση και η εκπαίδευση σχετικά με τον κίνδυνο ΤΠΕ να αποτελούν μέρος του μοντέλου διακυβέρνησης. Η παρούσα πολιτική διασφαλίζει ότι ο ανθρώπινος κίνδυνος αντιμετωπίζεται μέσω συνεχιζόμενης εκπαίδευσης και προσομοίωσης απειλών.

11.6.2 Άρθρα 5 και 8: Τονίζουν τη σημασία των πλαισίων εσωτερικού ελέγχου, των οποίων η ευαισθητοποίηση και η εκπαίδευση αποτελούν θεμελιώδη στοιχεία για την ανθεκτικότητα των ΤΠΕ και την κυβερνοϋγιεινή.

11.7 COBIT 2019

11.7.1 APO07 – Managed Human Resources: Ενισχύει την ανάγκη ανάπτυξης επίγνωσης των αρμοδιοτήτων ασφάλειας και ενσωμάτωσής της στη διαχείριση του ανθρώπινου δυναμικού.

11.7.2 DSS05 – Managed Security Services: Καθορίζει ελέγχους για την εκπαίδευση χρηστών και την αναφορά περιστατικών, που αμφότερα αποτελούν αναπόσπαστο μέρος της παρούσας πολιτικής.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Απαιτεί ανασκόπηση της αποτελεσματικότητας της συμπεριφοράς των χρηστών και της τήρησης της πολιτικής, η οποία εφαρμόζεται εδώ μέσω δοκιμών phishing, δοκιμασιών και δεικτών εκστρατειών ευαισθητοποίησης.