					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P08S					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	
ISO/IEC 27002:2022	Έλεγχος 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(i)	
Κανονισμός DORA της ΕΕ	Άρθρο 13	
COBIT 2019	BAI08, DSS	
ΓΚΠΔ της ΕΕ	Άρθρα 32, 39	

1. Σκοπός

1.1. Η παρούσα πολιτική διασφαλίζει ότι όλοι οι εργαζόμενοι και οι ανάδοχοι κατανοούν τις αρμοδιότητές τους σε σχέση με την ασφάλεια πληροφοριών.

1.2. Σκοπός της είναι η μείωση της πιθανότητας ανθρώπινου σφάλματος, η ενίσχυση της ικανότητας εντοπισμού και αναφοράς περιστατικών και η καλλιέργεια κουλτούρας ευαισθητοποίησης σε θέματα ασφάλειας σε ολόκληρο τον οργανισμό.

1.3. Η πολιτική υποστηρίζει τη συμμόρφωση με τα ISO/IEC 27001, NIS2, ΓΚΠΔ και DORA, ενσωματώνοντας την ευαισθητοποίηση σε θέματα ασφάλειας στην καθημερινή εργασιακή συμπεριφορά και στις προσδοκίες που συνδέονται με κάθε ρόλο.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε όλους τους εργαζομένους, αναδόχους, ασκούμενους και τρίτα μέρη που έχουν πρόσβαση σε συστήματα ή δεδομένα της εταιρείας.

2.2. Περιλαμβάνει:

2.2.1. Αρχική εκπαίδευση ευαισθητοποίησης για την ασφάλεια κατά την ένταξη νέου προσωπικού

2.2.2. Ετήσια επαναληπτική εκπαίδευση ασφάλειας

2.2.3. Έκτακτη εκπαίδευση και δράσεις ευαισθητοποίησης (π.χ. ενημερώσεις σχετικές με περιστατικά, αφίσες ή σύντομες συμβουλές)

2.3. Εφαρμόζεται σε όλους τους εργασιακούς ρόλους, τα τμήματα και τις τοποθεσίες εργασίας.

3. Στόχοι

3.1. Να διασφαλίζεται ότι όλο το προσωπικό λαμβάνει έγκαιρη, κατανοητή και συναφή εκπαίδευση ευαισθητοποίησης σε θέματα ασφάλειας.

3.2. Να παρέχεται στους εργαζομένους η δυνατότητα να αναγνωρίζουν και να αποφεύγουν συνήθεις απειλές, όπως το ηλεκτρονικό ψάρεμα, το κακόβουλο λογισμικό και οι διαρροές δεδομένων.

3.3. Να τηρείται τεκμηρίωση της ολοκλήρωσης της εκπαίδευσης, ώστε να αποδεικνύεται η συμμόρφωση με νομικές, συμβατικές και ελεγκτικές απαιτήσεις.

3.4. Να διατηρείται επικαιροποιημένο εκπαιδευτικό περιεχόμενο που αντανακλά τις πολιτικές του οργανισμού, το τοπίο απειλών και τις ισχύουσες κανονιστικές απαιτήσεις.

3.5. Να ενισχύεται προληπτική νοοτροπία στο προσωπικό, ώστε η ασφάλεια να αντιμετωπίζεται ως μέρος της καθημερινής ευθύνης.

4. Ρόλοι και αρμοδιότητες

4.1. Γενικός Διευθυντής

4.1.1. Εγκρίνει τις απαιτήσεις εκπαίδευσης και διασφαλίζει τη διάθεση των απαραίτητων πόρων.

4.1.2. Ανασκοπεί τις αναφορές ολοκλήρωσης και κλιμακώνει περιπτώσεις μη συμμόρφωσης, όπου απαιτείται.

4.2. Υπεύθυνος Διοικητικής Υποστήριξης / Ανθρώπινο Δυναμικό

4.2.1. Συντονίζει την παροχή εκπαίδευσης για τους νεοπροσλαμβανόμενους και την ετήσια επαναληπτική εκπαίδευση.

4.2.2. Τηρεί τα αρχεία εκπαίδευσης και τα σχετικά αρχεία καταγραφής ολοκλήρωσης.

4.2.3. Διασφαλίζει την επιβεβαίωση αποδοχής από το προσωπικό των βασικών πολιτικών ασφάλειας και των συμφωνιών εμπιστευτικότητας.

[... 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. Ετήσια ανασκόπηση

9.1.1. Η παρούσα πολιτική πρέπει να ανασκοπείται ετησίως από τον Γενικό Διευθυντή και το Ανθρώπινο Δυναμικό, ώστε να αντανακλά τους τρέχοντες κινδύνους, τις κανονιστικές απαιτήσεις και τις ανάγκες του προσωπικού.

9.2. Ενδιάμεσες επικαιροποιήσεις

9.2.1. Η πολιτική και το εκπαιδευτικό περιεχόμενο πρέπει επίσης να ανασκοπούνται και να αναθεωρούνται μετά από:

9.2.1.1. Σημαντικό περιστατικό ασφάλειας

9.2.1.2. Νομικές ή συμβατικές αλλαγές

9.2.1.3. Αναδιοργάνωση του οργανισμού ή μετεγκαταστάσεις συστημάτων

9.3. Έλεγχος εκδόσεων και διανομή

9.3.1. Κάθε επικαιροποίηση πρέπει να περιλαμβάνει:

9.3.1.1. Αριθμό έκδοσης και ημερομηνία έναρξης ισχύος

9.3.1.2. Σύνοψη αλλαγών

9.3.1.3. Έγκριση από τον Γενικό Διευθυντή

9.3.1.4. Αρχείο όλων των προηγούμενων εκδόσεων, το οποίο τηρείται για τουλάχιστον τρία έτη

9.4. Ενημέρωση εργαζομένων

9.4.1. Οι επικαιροποιήσεις της πολιτικής πρέπει να κοινοποιούνται σε όλο το προσωπικό και να λαμβάνεται επιβεβαίωση αποδοχής, εφόσον έχουν πραγματοποιηθεί ουσιώδεις αλλαγές.

10. Σχετικές πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική υποστηρίζει τα ακόλουθα:

10.1.1. P2S – Πολιτική ρόλων και αρμοδιοτήτων διακυβέρνησης: αναθέτει την ευθύνη για τον συντονισμό και την εποπτεία της εκπαίδευσης

10.1.2. P3S – Πολιτική Αποδεκτής Χρήσης: ενισχύει τις προσδοκίες συμπεριφοράς που καλύπτονται από την εκπαίδευση

10.1.3. P4S – Πολιτική Ελέγχου Πρόσβασης: διασφαλίζει ότι οι χρήστες κατανοούν τη σημασία της ασφάλειας πρόσβασης

10.1.4. P7S – Πολιτική Ένταξης και Αποχώρησης: ενσωματώνει την εκπαίδευση στη διαδικασία ένταξης

10.1.5. P30S – Πολιτική αντιμετώπισης περιστατικών: διασφαλίζει ότι το προσωπικό γνωρίζει πώς να αναφέρει περιστατικά έγκαιρα και ορθά

11. Πρότυπα και πλαίσια αναφοράς

11.1. ISO/IEC 27001

11.1.1. Ρήτρα 7.3 – Απαιτεί από τους οργανισμούς να διασφαλίζουν ότι το προσωπικό γνωρίζει τις αρμοδιότητές του και τις επιπτώσεις στην ασφάλεια

11.2. ISO/IEC 27002

11.2.1. Έλεγχος 6.3 – Περιγράφει τις απαιτήσεις για το πεδίο εφαρμογής και την παροχή εκπαίδευσης ασφάλειας

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – Απαιτεί εκπαίδευση ευαισθητοποίησης για χρήστες με πρόσβαση σε συστήματα

11.3.2. AT-4 – Καλύπτει την εκπαίδευση βάσει ρόλων και τις συνέπειες μη συμμόρφωσης

11.4. ΓΚΠΔ της ΕΕ

11.4.1. Άρθρο 32 – Επιβάλλει μέτρα ασφάλειας, συμπεριλαμβανομένης της εκπαίδευσης του προσωπικού, για την προστασία δεδομένων προσωπικού χαρακτήρα

11.4.2. Άρθρο 39 – Απαιτεί από τους Υπευθύνους Προστασίας Δεδομένων να ασκούν εποπτεία επί της ευαισθητοποίησης και της εκπαίδευσης, όπου εφαρμόζεται

11.5. Οδηγία NIS2 της ΕΕ

11.5.1. Άρθρο 21(2)(i) – Απαιτεί συνεχή προγράμματα ευαισθητοποίησης και εκπαίδευσης στην κυβερνοασφάλεια

11.6. Κανονισμός DORA της ΕΕ

11.6.1. Άρθρο 13 – Απαιτεί από τις χρηματοοικονομικές οντότητες να εφαρμόζουν εκπαίδευση και κατάρτιση για όλο το προσωπικό με αρμοδιότητες σχετικές με τις ΤΠΕ

11.7. COBIT 2019

11.7.1. BAI08 – Διαχείριση Γνώσης: διασφαλίζει ότι το προσωπικό είναι κατάλληλα καταρτισμένο και εκπαιδευμένο

11.7.2. DSS05 – Διαχείριση Υπηρεσιών Ασφάλειας: αναδεικνύει την ευαισθητοποίηση ως βασικό προληπτικό έλεγχο