1. ΣΚΟΠΟΣ

Η παρούσα Πολιτική Ασφάλειας Πληροφοριών εκφράζει τη δέσμευση της Διοίκησης της Αναπτυξιακή Κρήτης (ΑΝΚ) για τη διαφύλαξη της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών που διαχειρίζεται η εταιρεία, στο πλαίσιο του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) που εφαρμόζει σύμφωνα με το ISO/IEC 27001:2022.

2. ΠΕΡΙΓΡΑΦΗ

2.1 Πεδίο Εφαρμογής

Η παρούσα πολιτική εφαρμόζεται σε:

- Όλο το προσωπικό της ΑΝΚ, ανεξαρτήτως σχέσης εργασίας.
- Τους συνεργάτες, προμηθευτές και τρίτους που έχουν πρόσβαση σε πληροφορίες ή συστήματα της ΑΝΚ.
- Το σύνολο των πληροφοριακών συστημάτων, υποδομών ΤΠΕ και φυσικών εγκαταστάσεων της έδρας και τυχόν παραρτημάτων.
- Τη διαχείριση ευρωπαϊκών και εθνικών αναπτυξιακών προγραμμάτων που υποστηρίζει η ΑΝΚ.

Τυχόν εξαιρέσεις από το πεδίο εφαρμογής τεκμηριώνονται και αιτιολογούνται αποκλειστικά στη Δήλωση Εφαρμοστικότητας — SoA (Παράρτημα Α του ΕΓΧ-200).

2.2 Νομικό & Κανονιστικό Πλαίσιο

Η πολιτική διαμορφώνεται με βάση το ακόλουθο πλαίσιο:

- Κανονισμός (ΕΕ) 2016/679 — Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR).
- Ν. 4624/2019 — Μέτρα εφαρμογής του ΓΚΠΔ και αρμοδιότητες ΑΠΔΠΧ.
- Οδηγία NIS2 (ΕΕ 2022/2555) και η εθνική νομοθεσία ενσωμάτωσης, εφόσον εφαρμόζεται.
- Ν. 4727/2020 — Ψηφιακή Διακυβέρνηση.
- Ν. 4808/2021 — Πρόληψη και καταπολέμηση της βίας και παρενόχλησης στην εργασία, στο μέτρο που σχετίζεται με την ασφάλεια του προσωπικού.
- Κανονισμοί ΕΕ Διαρθρωτικών και Επενδυτικών Ταμείων 2021–2027 και ειδικές απαιτήσεις ασφάλειας των Διαχειριστικών Αρχών/ΔΥΠΑ.
- ISO/IEC 27001:2022, ISO/IEC 27002:2022 και ISO/IEC 27005:2022.

2.3 Δήλωση Πολιτικής Ασφάλειας Πληροφοριών

Η Διοίκηση της ΑΝΚ δηλώνει και δεσμεύεται ότι:

- Η ασφάλεια πληροφοριών αποτελεί αναπόσπαστο μέρος της στρατηγικής κατεύθυνσης και της καθημερινής λειτουργίας της εταιρείας.
- Η εταιρεία δεσμεύεται να καλύπτει όλες τις εφαρμοστέες νομικές, κανονιστικές και συμβατικές απαιτήσεις ασφάλειας πληροφοριών.
- Καθορίζονται και παρακολουθούνται στόχοι ασφάλειας πληροφοριών, συνεπείς με την παρούσα πολιτική.

- Διατίθενται οι αναγκαίοι ανθρώπινοι, τεχνολογικοί και οικονομικοί πόροι για την εγκαθίδρυση, λειτουργία και βελτίωση του ΣΔΑΠ.
- Η εταιρεία δεσμεύεται για τη συνεχή βελτίωση του ΣΔΑΠ, μέσω τακτικής παρακολούθησης, εσωτερικών ελέγχων και Ανασκοπήσεων Διοίκησης.
- Οι αρμοδιότητες ασφάλειας πληροφοριών ανά ρόλο είναι καθορισμένες, τεκμηριωμένες και γνωστές σε όλο το προσωπικό.
- Κάθε παρέκκλιση ή εξαίρεση από την πολιτική αντιμετωπίζεται σύμφωνα με την επίσημη διαδικασία διαχείρισης εξαιρέσεων (βλ. Ενότητα 8).

Η παρούσα πολιτική εγκρίνεται από τη Διοίκηση, καταγράφεται και τηρείται ως έγγραφο, κοινοποιείται σε όλο το προσωπικό και τα ενδιαφερόμενα μέρη όπου κρίνεται σκόπιμο, και είναι διαθέσιμη μέσω της ιστοσελίδας της εταιρείας (www.ank.gr).

2.4 Στόχοι Ασφάλειας Πληροφοριών

Η ΑΝΚ καθορίζει στόχους ασφάλειας πληροφοριών σε σχετικές λειτουργίες και επίπεδα, οι οποίοι:

- Είναι συνεπείς με την παρούσα πολιτική.
- Είναι μετρήσιμοι, όπου αυτό είναι εφικτό.
- Λαμβάνουν υπόψη τις εφαρμοστέες απαιτήσεις ασφάλειας πληροφοριών και τα αποτελέσματα της εκτίμησης/αντιμετώπισης κινδύνου.
- Παρακολουθούνται, κοινοποιούνται και επικαιροποιούνται όπως απαιτείται.

Οι στόχοι ασφάλειας πληροφοριών, οι σχετικοί δείκτες απόδοσης (KPIs), οι υπεύθυνοι υλοποίησης και τα χρονοδιαγράμματα τηρούνται και παρακολουθούνται στην πλατφόρμα ISOWise. Η πρόοδος επί των στόχων αποτελεί πάγιο θέμα των Ανασκοπήσεων Διοίκησης.●

2.5 Ειδικές Θεματικές Πολιτικές

Πέρα από την παρούσα κύρια πολιτική, η ΑΝΚ διατηρεί ξεχωριστές, πιο συγκεκριμένες πολιτικές για:

- Έλεγχο πρόσβασης.
- Ταξινόμηση πληροφοριών.
- Αντίγραφα ασφαλείας.
- Καθαρό γραφείο / καθαρή οθόνη.
- Τηλεργασία.
- Κρυπτογράφηση.
- Αποδεκτή χρήση πόρων ΤΠΕ.
- Διαχείριση περιστατικών ασφάλειας.

Κάθε θεματική πολιτική εγκρίνεται από τη Διοίκηση και κοινοποιείται σε όσους αφορά.

2.6 Ρόλοι & Αρμοδιότητες

Η Διοίκηση φροντίζει ώστε οι αρμοδιότητες ασφάλειας πληροφοριών να είναι καθορισμένες και γνωστές σε όλους. Ο αναλυτικός πίνακας ρόλων και αρμοδιοτήτων παρατίθεται στο Παράρτημα Γ του ΕΓΧ-200.

Συνοπτικά:

Ρόλος	Κύρια Αρμοδιότητα
Διοίκηση / Διευθύνων Σύμβουλος	Τελική ευθύνη ΣΔΑΠ, έγκριση πολιτικών και πόρων, πρόεδρος Ανασκόπησης Διοίκησης.
CISO (Υπεύθυνος Ασφάλειας Πληροφοριών)	Διαχείριση, συντονισμός και αποτελεσματικότητα του ΣΔΑΠ, σύνταξη εκθέσεων προς τη Διοίκηση.
IT Manager / Υπεύθυνος Μηχανογράφησης	Τεχνική υλοποίηση των ελέγχων Annex A κατηγορίας 8, διαχείριση υποδομών ΤΠΕ.
DPO (Υπεύθυνος Προστασίας Δεδομένων)	Συμμόρφωση με το GDPR, σύνδεσμος με την ΑΠΔΠΧ.
Ιδιοκτήτες Περιουσιακών Στοιχείω (Asset Owners)	Ταξινόμηση, προστασία και διαχείριση του κύκλου ζωής των στοιχείων ευθύνης τους. Καταγράφονται στο ISOWise.
Όλο το Προσωπικό & Συνεργάτες	Συμμόρφωση με τις πολιτικές ασφάλειας, αναφορά συμβάντων ή υπόνοιας συμβάντων.

2.7 Διαχείριση Εξαιρέσεων

Οποιαδήποτε παρέκκλιση από την παρούσα πολιτική ή τις επιμέρους θεματικές πολιτικές πρέπει να τεκμηριώνεται και να εγκρίνεται εκ των προτέρων από τον CISO, με ενημέρωση της Διοίκησης όπου η εξαίρεση αφορά ουσιώδη μεταβολή κινδύνου. Οι εξαιρέσεις που αφορούν ελέγχους του Annex A τεκμηριώνονται αποκλειστικά στη Δήλωση Εφαρμοστικότητας (SoA — Παράρτημα Α του ΕΓΧ-200), μαζί με την αιτιολόγησή τους μέσω εκτίμησης κινδύνου.

2.8 Επανεξέταση Πολιτικής

Η παρούσα πολιτική επανεξετάζεται τουλάχιστον μία φορά τον χρόνο, καθώς και επιπλέον όποτε γίνεται σημαντική αλλαγή, όπως:

- Αλλαγή στη νομοθεσία ή στο κανονιστικό πλαίσιο.
- Σημαντικό περιστατικό ασφάλειας πληροφοριών.
- Νέο εύρημα από εσωτερικό έλεγχο.
- Αλλαγή στο πλαίσιο λειτουργίας της εταιρείας.

Υπεύθυνος για την επανεξέταση είναι ο CISO, με τελική έγκριση από τη Διοίκηση.

2.9 Ισχύς & Κοινοποίηση

Η παρούσα πολιτική τίθεται σε ισχύ από την ημερομηνία έγκρισής της, κοινοποιείται σε όλο το προσωπικό και τους συνεργάτες της ANK, και είναι διαθέσιμη στα ενδιαφερόμενα μέρη μέσω της ιστοσελίδας www.ank.gr. Η μη συμμόρφωση με την παρούσα πολιτική μπορεί να επισύρει πειθαρχικές συνέπειες, σύμφωνα με τις ισχύουσες διαδικασίες της εταιρείας.