					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P01S					Τίτλος εγγράφου: **Πολιτική Ασφάλειας 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 κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο/Έλεγχος	Σχόλιο
ISO/IEC 27001:2022	Ρήτρες 5.1, 5.2, 5.3, 6.1, 6.2, 8	Καθορίζει τη δέσμευση της διοίκησης, τις απαιτήσεις της πολιτικής, την ανάθεση ρόλων, την αξιολόγηση κινδύνων και τον επιχειρησιακό έλεγχο
ISO/IEC 27002:2022	Έλεγχοι 5.1–5.4	Καθορίζει τη θέσπιση τεκμηριωμένων πολιτικών ασφάλειας πληροφοριών, την ανάθεση ρόλων, τον διαχωρισμό καθηκόντων και τις αρμοδιότητες της διοίκησης
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Περιλαμβάνει απαιτήσεις για το σχέδιο προγράμματος ασφάλειας πληροφοριών, την πολιτική σχεδιασμού ασφάλειας, την αξιολόγηση/εξουσιοδότηση και τον έλεγχο πρόσβασης
ΓΚΠΔ της ΕΕ (2016/679)	Άρθρο 5(2), Άρθρο 32	Καθιερώνει την αρχή της λογοδοσίας και απαιτεί μέτρα για την ασφάλεια της επεξεργασίας, ιδίως ως προς τους τεκμηριωμένους ρόλους
Οδηγία NIS2 της ΕΕ (2022/2555)	Άρθρο 21(2)(a)	Απαιτεί μέτρα διαχείρισης κινδύνων, καθώς και σαφείς ρόλους και αρμοδιότητες για τη διαχείριση κυβερνοκινδύνων
Κανονισμός DORA της ΕΕ (2022/2554)	Άρθρο 9, Άρθρο 10	Απαιτεί την ανάθεση ρόλων για τη διαχείριση κινδύνων ΤΠΕ και τη διασφάλιση της επιχειρησιακής συνέχειας
COBIT 2019	EDM03, APO13, DSS05	Διασφαλίζει τη βελτιστοποίηση κινδύνου, τη διαχείριση της ασφάλειας και τη διαχείριση υπηρεσιών ασφάλειας μέσω σαφούς ανάθεσης ρόλων

1. Σκοπός

1.1 Η παρούσα πολιτική αποτυπώνει τη δέσμευση του οργανισμού να προστατεύει τις πληροφορίες πελατών και τις επιχειρησιακές πληροφορίες μέσω σαφώς καθορισμένων αρμοδιοτήτων και πρακτικών μέτρων ασφαλείας, κατάλληλων για οργανισμούς χωρίς εξειδικευμένες ομάδες πληροφορικής.

1.2 Διασφαλίζει ότι όλοι οι εργαζόμενοι, οι ανάδοχοι και οι πάροχοι υπηρεσιών τηρούν υποχρεωτικούς κανόνες, ώστε να επιτυγχάνεται πλήρης συμμόρφωση με τις απαιτήσεις πιστοποίησης του ISO/IEC 27001.

1.3 Η παρούσα πολιτική συμβάλλει στην ενίσχυση της εμπιστοσύνης των πελατών, αποδεικνύοντας με σαφήνεια τον τρόπο με τον οποίο προστατεύονται οι πληροφορίες τους μέσω καθορισμένων αρμοδιοτήτων, δομημένων διαδικασιών και ισχυρής λογοδοσίας.

2. Πεδίο εφαρμογής

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

2.1.1 Ιδιοκτήτες της επιχείρησης και γενικοί διευθυντές

2.1.2 Εργαζόμενοι, ανάδοχοι και ασκούμενοι

2.1.3 Εξωτερικοί πάροχοι υπηρεσιών πληροφορικής ή σύμβουλοι

2.2 Καλύπτει όλες τις κατηγορίες πληροφοριών, συστημάτων και υπηρεσιών, συμπεριλαμβανομένων των εξής:

2.2.1 Επιχειρησιακά αρχεία, δεδομένα πελατών, κωδικοί πρόσβασης και μηνύματα ηλεκτρονικού ταχυδρομείου

2.2.2 Εξοπλισμός πληροφορικής, όπως φορητοί υπολογιστές και τηλέφωνα

2.2.3 Υπηρεσίες υπολογιστικού νέφους που χρησιμοποιούνται για αποθήκευση αρχείων, επικοινωνία ή οικονομική διαχείριση

2.2.4 Φυσικά έγγραφα που φυλάσσονται στους χώρους γραφείου

2.3 Η πολιτική εφαρμόζεται σε όλα τα περιβάλλοντα εργασίας — σε χώρους γραφείου, σε καθεστώς τηλεργασίας και σε περιβάλλον υπολογιστικού νέφους — και καλύπτει όλες τις συσκευές και το λογισμικό που χρησιμοποιούνται για την επεξεργασία ή την αποθήκευση επιχειρησιακών πληροφοριών.

3. Στόχοι

3.1 Σαφής ανάθεση ευθύνης: Να διασφαλίζεται ότι υπάρχει πάντοτε σαφώς ορισμένο πρόσωπο με ευθύνη και λογοδοσία για την ασφάλεια πληροφοριών. Συνήθως πρόκειται για τον Γενικό Διευθυντή ή το πρόσωπο που αυτός ορίζει επισήμως.

3.2 Προστασία πληροφοριών πελατών και επιχειρησιακών πληροφοριών: Να παρέχονται αξιόπιστες και συνεπείς δικλίδες ασφαλείας για την αποτροπή κακής χρήσης, απώλειας ή κλοπής ευαίσθητων δεδομένων, συμπεριλαμβανομένων αρχείων πελατών και οικονομικών αρχείων.

3.3 Υποστήριξη της πιστοποίησης ISO/IEC 27001: Να επιτρέπεται στον οργανισμό να αποδεικνύει πλήρη συμμόρφωση με τις απαιτήσεις του ISO/IEC 27001, διασφαλίζοντας ετοιμότητα ελέγχου και καταλληλότητα για πιστοποίηση χωρίς ανάγκη σύνθετης υποδομής.

3.4 Ενσωμάτωση της ασφάλειας στις επιχειρησιακές λειτουργίες: Να ενσωματώνεται η ασφάλεια πληροφοριών στις καθημερινές εργασίες και αποφάσεις σε όλο τον οργανισμό.

3.5 Καλλιέργεια ευαισθητοποίησης και κουλτούρας ασφάλειας: Να ενθαρρύνεται κάθε εργαζόμενος να κατανοεί και να τηρεί τις πρακτικές ασφάλειας, όπως η χρήση ισχυρών κωδικών πρόσβασης και η αναφορά ύποπτης δραστηριότητας.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής ή ιδιοκτήτης της επιχείρησης

4.1.1 Φέρει τη συνολική ευθύνη και λογοδοσία για την ασφάλεια πληροφοριών.

4.1.2 Εγκρίνει και διατηρεί σε ισχύ την παρούσα πολιτική.

4.1.3 Διασφαλίζει ότι όλα τα βασικά καθήκοντα ασφάλειας πληροφοριών είτε εκτελούνται απευθείας είτε ανατίθενται γραπτώς.

4.1.4 Επαληθεύει ότι κάθε ανατεθειμένο καθήκον ασφάλειας πληροφοριών (όπως η διαχείριση πρόσβασης ή η αντιμετώπιση περιστατικών) εκτελείται αποτελεσματικά.

4.1.5 Αποτελεί το κύριο σημείο επαφής για όλα τα εσωτερικά και εξωτερικά θέματα ασφάλειας, συμπεριλαμβανομένων ελέγχων και ερωτημάτων πελατών.

4.1.6 Παρακολουθεί, στο πλαίσιο της ετήσιας ανασκόπησης, την πρόοδο έναντι των στόχων της παρούσας πολιτικής. Οι στόχοι πρέπει, όπου είναι εφικτό, να είναι μετρήσιμοι (π.χ. ποσοστό προσωπικού που έχει εκπαιδευτεί, αριθμός περιστατικών που έχουν αναφερθεί κ.λπ.) και να επικαιροποιούνται βάσει ευρημάτων ασφάλειας και μεταβολών του κινδύνου.

4.2 Ορισμένος εργαζόμενος (κατά περίπτωση)

4.2.1 Μπορεί να υποστηρίζει τον Γενικό Διευθυντή στη διαχείριση καθημερινών εργασιών, όπως η δημιουργία λογαριασμών χρηστών, η αφαίρεση δικαιωμάτων πρόσβασης για αποχωρούντες εργαζόμενους ή ο συντονισμός με τον εξωτερικό πάροχο υπηρεσιών πληροφορικής.

4.2.2 Πρέπει να ορίζεται επισήμως και να διαθέτει την απαραίτητη εξουσιοδότηση και τα κατάλληλα εργαλεία για την εκτέλεση των καθηκόντων του.

4.2.3 Αναφέρει κάθε σχετικό ζήτημα στον Γενικό Διευθυντή.

[... 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 από τον Γενικό Διευθυντή τουλάχιστον μία φορά ετησίως, ώστε να διασφαλίζεται η διαρκής συμμόρφωση με τις απαιτήσεις πιστοποίησης του ISO/IEC 27001, τις κανονιστικές μεταβολές (όπως ο ΓΚΠΔ της ΕΕ, η Οδηγία NIS2 της ΕΕ και ο Κανονισμός DORA της ΕΕ) και τις μεταβαλλόμενες επιχειρησιακές ανάγκες.

9.2 Ενδιάμεσες ανασκοπήσεις

9.2.1 Πρόσθετες ανασκοπήσεις πρέπει να πραγματοποιούνται όποτε προκύπτουν σημαντικές αλλαγές, όπως:

9.2.1.1 Μείζονα περιστατικά ασφάλειας ή παραβιάσεις

9.2.1.2 Εισαγωγή νέων επιχειρησιακών διεργασιών ή τεχνολογιών (π.χ. νέο λογισμικό, πλατφόρμες τηλεργασίας ή υπηρεσίες υπολογιστικού νέφους)

9.2.1.3 Μεταβολές στις νομικές ή κανονιστικές απαιτήσεις που επηρεάζουν τον χειρισμό πληροφοριών

9.3 Τεκμηρίωση αλλαγών

9.3.1 Όλες οι ανασκοπήσεις και οι αλλαγές της πολιτικής πρέπει να τεκμηριώνονται επισήμως, με σαφή αναφορά στην ημερομηνία, στο είδος των αναθεωρήσεων και στην έγκριση του Γενικού Διευθυντή.

9.3.2 Πρέπει να τηρείται με ασφάλεια ιστορικό εκδόσεων της πολιτικής, ώστε να αποδεικνύεται η εξέλιξή της και η συμμόρφωση κατά τους ελέγχους.

9.4 Κοινοποίηση επικαιροποιήσεων

9.4.1 Κάθε αλλαγή στην παρούσα πολιτική πρέπει να κοινοποιείται άμεσα σε όλους τους εργαζομένους, τους αναδόχους και τα σχετικά τρίτα μέρη.

9.4.2 Οι επικαιροποιημένες εκδόσεις της πολιτικής πρέπει να είναι εύκολα προσβάσιμες σε όλο το επηρεαζόμενο προσωπικό (π.χ. να κοινοποιούνται ηλεκτρονικά ή να αναρτώνται στους χώρους εργασίας).

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική συνδέεται στενά με άλλες πολιτικές του πλαισίου πολιτικών ΜΜΕ του οργανισμού και ειδικότερα με τις εξής:

10.1.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Αποσαφηνίζει την ανάθεση καθηκόντων και αρμοδιοτήτων ασφάλειας.

10.1.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Ορίζει την ασφαλή διαχείριση της πρόσβασης στις πληροφορίες του οργανισμού.

10.1.3 P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Παρέχει βασικές κατευθύνσεις για την εκπαίδευση και την ευαισθητοποίηση του προσωπικού.

10.1.4 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Διασφαλίζει τη συμμόρφωση με τον ΓΚΠΔ της ΕΕ και άλλους νόμους προστασίας δεδομένων.

10.1.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Περιγράφει αναλυτικά τις ενέργειες που απαιτούνται για την αντιμετώπιση περιστατικών ασφάλειας.

10.2 Οι συναφείς αυτές πολιτικές παρέχουν σαφή επιχειρησιακή καθοδήγηση και πρέπει να εφαρμόζονται συνδυαστικά για την επίτευξη πλήρους συμμόρφωσης με τις απαιτήσεις πιστοποίησης του ISO/IEC 27001.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001:2022

11.1.1 Ρήτρα 5.1 – Ηγεσία και δέσμευση: Απαιτεί τη δέσμευση της ανώτατης διοίκησης και τη λογοδοσία για την αποτελεσματικότητα της ασφάλειας πληροφοριών σε όλο τον οργανισμό.

11.1.2 Ρήτρα 5.2 – Πολιτική ασφάλειας πληροφοριών: Απαιτεί σαφείς, τεκμηριωμένες πολιτικές ευθυγραμμισμένες με τη στρατηγική του οργανισμού και τις απαιτήσεις συμμόρφωσης.

11.1.3 Ρήτρα 5.3 – Οργανωτικοί ρόλοι και αρμοδιότητες: Ορίζει τη σαφή ανάθεση αρμοδιοτήτων ασφάλειας πληροφοριών σε όλο τον οργανισμό, ως ουσιώδες στοιχείο για αποτελεσματική διακυβέρνηση και ετοιμότητα ελέγχου.

11.1.4 Ρήτρα 6.1 – Ενέργειες για την αντιμετώπιση κινδύνων και ευκαιριών: Διασφαλίζει ότι οι κίνδυνοι για την ασφάλεια πληροφοριών αναγνωρίζονται, αξιολογούνται και αντιμετωπίζονται συστηματικά.

11.1.5 Ρήτρα 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί από τον οργανισμό να σχεδιάζει και να εφαρμόζει τις διεργασίες που απαιτούνται για την επίτευξη των στόχων ασφάλειας πληροφοριών και για την αποτελεσματική διαχείριση των συναφών κινδύνων.

11.2 Έλεγχοι 5.1–5.4 του ISO/IEC 27002:2022

11.2.1 Έλεγχος 5.1 του Παραρτήματος Α – Πολιτικές για την ασφάλεια πληροφοριών: Καθορίζει τη θέσπιση και την κοινοποίηση τεκμηριωμένων πολιτικών ασφάλειας πληροφοριών.

11.2.2 Έλεγχος 5.2 του Παραρτήματος Α – Ρόλοι ασφάλειας πληροφοριών: Αποσαφηνίζει και αναθέτει επισήμως τους ρόλους και τις αρμοδιότητες ασφάλειας πληροφοριών στα αρμόδια μέρη.

11.2.3 Έλεγχος 5.3 του Παραρτήματος Α – Διαχωρισμός καθηκόντων: Επιβάλλει σαφή διαχωρισμό καθηκόντων για τη μείωση συγκρούσεων συμφερόντων και κινδύνων απάτης κατά τη διαχείριση ευαίσθητων πληροφοριών.

11.2.4 Έλεγχος 5.4 του Παραρτήματος Α – Αρμοδιότητες της διοίκησης: Απαιτεί από τη διοίκηση να αποδεικνύει δέσμευση στην ασφάλεια πληροφοριών μέσω ενεργής εποπτείας και διάθεσης πόρων.

11.2.5 Οι έλεγχοι αυτοί ενισχύουν την αναγκαιότητα σαφώς τεκμηριωμένων πολιτικών, ρόλων, αρμοδιοτήτων και δομών διακυβέρνησης για την ασφάλεια πληροφοριών, διασφαλίζοντας συνεπή διαχείριση και ιχνηλασιμότητα για σκοπούς ελέγχου σε όλο τον οργανισμό.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Σχέδιο Προγράμματος Ασφάλειας Πληροφοριών: Απαιτεί τεκμηριωμένες στρατηγικές διακυβέρνησης της ασφάλειας πληροφοριών και σχετικές πολιτικές, παρέχοντας πλαίσιο για συνεπή εφαρμογή και διαχείριση.

11.3.2 PL-1 – Πολιτική Σχεδιασμού Ασφάλειας: Απαιτεί πολιτική σχεδιασμού ασφάλειας σε επίπεδο οργανισμού, ώστε να καθοδηγείται η ασφαλής λειτουργία και η στρατηγική ευθυγράμμιση των δραστηριοτήτων ασφάλειας πληροφοριών.

11.3.3 CA-1 – Πολιτική Αξιολόγησης και Εξουσιοδότησης Ασφάλειας: Απαιτεί σαφώς καθορισμένους ρόλους αξιολόγησης και εξουσιοδότησης, ώστε να διασφαλίζεται η συνεχής αποτελεσματικότητα και συμμόρφωση με τις απαιτήσεις ασφάλειας πληροφοριών.

11.3.4 AC-1 – Πολιτική Ελέγχου Πρόσβασης: Απαιτεί από τους οργανισμούς να ορίζουν, να τεκμηριώνουν και να εφαρμόζουν σαφώς τις πρακτικές και τις αρμοδιότητες διαχείρισης πρόσβασης.

11.4 ΓΚΠΔ της ΕΕ (2016/679)

11.4.1 Άρθρο 5(2) – Αρχή λογοδοσίας: Απαιτεί από τους οργανισμούς να αποδεικνύουν συμμόρφωση με τις αρχές προστασίας δεδομένων, συμπεριλαμβανομένων τεκμηριωμένων ρόλων και πολιτικών για τις αρμοδιότητες προστασίας δεδομένων.

11.4.2 Άρθρο 32 – Ασφάλεια της επεξεργασίας: Απαιτεί την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, συμπεριλαμβανομένων σαφών αρμοδιοτήτων ασφάλειας, για την προστασία των δεδομένων προσωπικού χαρακτήρα από παραβιάσεις και μη εξουσιοδοτημένη πρόσβαση.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(a) – Μέτρα διαχείρισης κινδύνων: Απαιτεί σαφείς ρυθμίσεις διακυβέρνησης, συμπεριλαμβανομένων καθορισμένων ρόλων και αρμοδιοτήτων για την ασφάλεια πληροφοριών, οι οποίες είναι ουσιώδεις για την αποτελεσματική διαχείριση κυβερνοκινδύνων.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 9 – Διαχείριση κινδύνων ΤΠΕ: Απαιτεί από τους οργανισμούς να αναθέτουν με σαφήνεια τους ρόλους και τις αρμοδιότητες που σχετίζονται με τη διαχείριση κινδύνων ΤΠΕ, ενισχύοντας την ανθεκτικότητα και την ετοιμότητα για επιχειρησιακή συνέχεια.

11.6.2 Άρθρο 10 – Επιχειρησιακή συνέχεια ΤΠΕ: Απαιτεί σαφή λογοδοσία και δομημένους ρόλους για τη διατήρηση της ανθεκτικότητας και της συνέχειας των ΤΠΕ, διασφαλίζοντας ότι οι οργανισμοί μπορούν να ανταποκρίνονται αξιόπιστα σε διαταραχές.

11.7 COBIT 2019

11.7.1 EDM03 – Διασφάλιση βελτιστοποίησης κινδύνου: Τονίζει τη σαφή λογοδοσία και τον σαφή καθορισμό ρόλων στη διαχείριση των κινδύνων του οργανισμού, παρέχοντας ισχυρή διακυβέρνηση και αποτελεσματική εποπτεία των κινδύνων ασφάλειας πληροφοριών.

11.7.2 APO13 – Διαχείριση ασφάλειας: Απαιτεί από τους οργανισμούς να καθορίζουν και να κοινοποιούν με σαφήνεια τις αρμοδιότητες διαχείρισης ασφάλειας, διασφαλίζοντας ευθυγράμμιση με επιχειρησιακούς στόχους και κανονιστικές απαιτήσεις.

11.7.3 DSS05 – Διαχείριση υπηρεσιών ασφάλειας: Προβλέπει δομημένους ρόλους και σαφείς αρμοδιότητες για τη διαχείριση υπηρεσιών ασφάλειας, επιτρέποντας συνεπή εφαρμογή και επαλήθευση της συμμόρφωσης.