					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P03					Τίτλος εγγράφου: **Πολιτική Αποδεκτής Χρήσης**							
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**	**Σχόλιο**
ISO/IEC 27001:2022	Ρήτρα 5	Καθορίζει κανόνες συμπεριφοράς και απαιτήσεις για την Πολιτική Αποδεκτής Χρήσης
ISO/IEC 27002:2022	Έλεγχοι 6.1, 6.2, 8.1, 8.12	Παρέχει κατευθύνσεις για τις ευθύνες ασφάλειας πληροφοριών, την ευαισθητοποίηση και τη διακυβέρνηση συσκευών/δεδομένων
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Έλεγχοι πρόσβασης και ευαισθητοποίησης/συμπεριφοράς που σχετίζονται με τη χρήση περιουσιακών στοιχείων ΤΠ
ΓΚΠΔ της ΕΕ	Άρθρα 5(1)(f), 32, Αιτιολογική σκέψη 39	Επιβάλλει την εμπιστευτικότητα και ακεραιότητα, απαιτεί τεχνικά και οργανωτικά μέτρα και νόμιμη βάση για την ορθή χρήση
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(a–d)	Απαιτεί επιχειρησιακές πολιτικές και εκπαίδευση για ασφαλή χρήση
Κανονισμός DORA της ΕΕ	Άρθρο 5	Υποστηρίζει τη διαχείριση κινδύνων ΤΠΕ μέσω της ρύθμισης της συμπεριφοράς των χρηστών
COBIT 2019	APO07, BAI05, DSS05, MEA01	Ανθρώπινο δυναμικό, διαχείριση αλλαγών, διαχειριζόμενη ασφάλεια, παρακολούθηση συμμόρφωσης/απόδοσης

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει την αποδεκτή και μη αποδεκτή χρήση των πληροφοριακών συστημάτων του οργανισμού, των υπολογιστικών πόρων, των εργαλείων επικοινωνίας και των πρακτικών διαχείρισης δεδομένων.

1.2 Διασφαλίζει ότι όλοι οι χρήστες κατανοούν τις ευθύνες τους κατά τη χρήση εταιρικών περιουσιακών στοιχείων ΤΠ και ότι οι ενέργειές τους υποστηρίζουν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και τη νόμιμη επεξεργασία των πληροφοριών.

1.3 Η πολιτική ικανοποιεί τη Ρήτρα 5.10 του ISO/IEC 27001:2022, καθορίζοντας κανόνες συμπεριφοράς για τη χρήση συστημάτων και εφαρμόζοντας τεχνικές και διαδικαστικές δικλίδες ασφαλείας για την ελαχιστοποίηση του κινδύνου κακής χρήσης, αμέλειας ή κατάχρησης.

1.4 Υποστηρίζει επίσης δραστηριότητες διερεύνησης και επιβολής της πολιτικής, συμπεριλαμβανομένης της απόκρισης σε περιστατικά και της επιβολής πειθαρχικών μέτρων για παραβάσεις.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα φυσικά πρόσωπα και τις οντότητες στα οποία έχει χορηγηθεί πρόσβαση στα πληροφοριακά συστήματα και τα περιουσιακά στοιχεία του οργανισμού, συμπεριλαμβανομένων ενδεικτικά των εξής:

2.1.1 Εργαζομένων, αναδόχων, συμβούλων, ασκουμένων και απασχολουμένων μέσω εταιρειών προσωρινής απασχόλησης

2.1.2 Προμηθευτών ή άλλων τρίτων με πρόσβαση σε συστήματα ή με εκχωρημένους διοικητικούς ρόλους

2.1.3 Επισκεπτών ή συνεργατών που χρησιμοποιούν ιδιόκτητη ή εγκεκριμένη υποδομή ΤΠ του οργανισμού

2.2 Το πεδίο εφαρμογής περιλαμβάνει όλα τα τεχνολογικά και πληροφοριακά περιουσιακά στοιχεία του οργανισμού, συμπεριλαμβανομένων των εξής:

2.2.1 Σταθμών εργασίας, φορητών υπολογιστών, κινητών συσκευών και διακομιστών

2.2.2 Δικτυακής υποδομής και υπηρεσιών που φιλοξενούνται σε υπολογιστικό νέφος

2.2.3 Ηλεκτρονικού ταχυδρομείου, ανταλλαγής μηνυμάτων, αποθήκευσης αρχείων, πλατφορμών συνεργασίας και VPN

2.2.4 Δεδομένων σε αποθήκευση, σε μεταφορά ή υπό επεξεργασία, ανεξαρτήτως μορφής ή τοποθεσίας

2.2.5 Οποιασδήποτε προσωπικής συσκευής χρησιμοποιείται στο πλαίσιο BYOD (Bring Your Own Device) και συνδέεται με συστήματα του οργανισμού

2.3 Η παρούσα πολιτική εφαρμόζεται σε όλα τα περιβάλλοντα εργασίας, συμπεριλαμβανομένων των εξής:

2.3.1 Εταιρικών γραφείων και εγκαταστάσεων παραγωγής

2.3.2 Τοποθεσιών απομακρυσμένης εργασίας ή υβριδικών σχημάτων εργασίας

2.3.3 Επιχειρησιακών δραστηριοτήτων πεδίου ή εγκαταστάσεων που διαχειρίζονται τρίτοι

2.4 Όλοι οι χρήστες οφείλουν να αναγνωρίζουν και να τηρούν την παρούσα πολιτική ως προϋπόθεση για την πρόσβαση σε εταιρικά συστήματα ή τον χειρισμό εταιρικών δεδομένων.

3. Στόχοι

3.1 Να καθορίζει και να επιβάλλει κανόνες για την αποδεκτή χρήση των πόρων ΤΠ του οργανισμού.

3.2 Να αποτρέπει μη εξουσιοδοτημένη πρόσβαση, διαρροή δεδομένων ή ζημία που προκύπτει από αμελή ή κακόβουλη χρήση.

3.3 Να προστατεύει τα εταιρικά δίκτυα, τα περιουσιακά στοιχεία και τα δεδομένα από απειλές που εισάγονται μέσω της συμπεριφοράς των χρηστών.

3.4 Να υποστηρίζει νομικές και συμβατικές υποχρεώσεις, αποδεικνύοντας τη δέουσα επιμέλεια στη διακυβέρνηση των πόρων ΤΠ.

3.5 Να διασφαλίζει συνέπεια και σαφήνεια στην επιβολή πειθαρχικών μέτρων και στις διαδικασίες διαχείρισης εξαιρέσεων.

3.6 Να προάγει κουλτούρα ηθικής, ασφαλούς και υπεύθυνης χρήσης ψηφιακών και φυσικών υπολογιστικών πόρων.

4. Ρόλοι και αρμοδιότητες

4.1 Ανώτατη Διοίκηση

4.1.1 Εγκρίνει την Πολιτική Αποδεκτής Χρήσης (AUP) και διασφαλίζει ότι ευθυγραμμίζεται με τους επιχειρησιακούς στόχους, τις κανονιστικές απαιτήσεις και τις αξίες του οργανισμού.

4.1.2 Διαθέτει τους απαιτούμενους πόρους για την εφαρμογή, την εκπαίδευση, την παρακολούθηση και την ανασκόπηση της πολιτικής.

4.1.3 Ανασκοπεί την κατάσταση συμμόρφωσης και τα πειθαρχικά μέτρα που σχετίζονται με παραβιάσεις της πολιτικής στο πλαίσιο της διακυβέρνησης του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS).

4.2 Ομάδες ΤΠ και Ασφάλειας Πληροφοριών

4.2.1 Υλοποιούν τεχνικές δικλίδες ασφαλείας για την εφαρμογή της παρούσας πολιτικής, συμπεριλαμβανομένων των εξής:

4.2.2 Φιλτραρίσματος περιεχομένου, προστασίας από κακόβουλο λογισμικό, ασφάλειας τερματικών σημείων και εργαλείων παρακολούθησης δικτύου

4.2.3 Ρυθμίσεων ασφάλειας ηλεκτρονικού ταχυδρομείου και λύσεων πρόληψης απώλειας δεδομένων (DLP)

4.2.4 Λιστών αποκλεισμού και λιστών επιτρεπόμενων για λογισμικό, υλικό και ιστοτόπους

4.2.5 Τηρούν απογραφή εγκεκριμένου και απαγορευμένου λογισμικού, συσκευών και υπηρεσιών.

4.2.6 Διερευνούν πιθανολογούμενες παραβιάσεις της AUP, συλλέγουν ψηφιακά πειστήρια και υποστηρίζουν πειθαρχικές ή νομικές ενέργειες, όπου ενδείκνυται.

4.2.7 Συνεργάζονται με τη Διεύθυνση Ανθρώπινου Δυναμικού και τη Νομική Υπηρεσία για τη διαχείριση περιστατικών, την κλιμάκωση και τις υποχρεώσεις αναφοράς.

[... 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 Εναύσματα και συχνότητα ανασκόπησης

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται:

9.1.1.1 Τουλάχιστον ετησίως

9.1.1.2 Μετά από κάθε σημαντική αλλαγή τεχνολογίας ή υποδομής

9.1.1.3 Μετά από περιστατικά ή ευρήματα ελέγχου που αναδεικνύουν κενά στην εφαρμογή

9.1.1.4 Σε απόκριση σε αλλαγές της εφαρμοστέας νομοθεσίας ή συμβάσεων

9.2 Κυριότητα και έγκριση

9.2.1 Ο CISO ή ο ορισμένος Υπεύθυνος ISMS είναι υπεύθυνος για τη διαδικασία ανασκόπησης.

9.2.2 Οι επικαιροποιήσεις πρέπει να εγκρίνονται από την Ανώτατη Διοίκηση και να κοινοποιούνται σε όλο τον οργανισμό.

9.2.3 Η αποδοχή των επικαιροποιημένων όρων πρέπει να λαμβάνεται εκ νέου με την επανέκδοση της πολιτικής.

9.3 Διαχείριση εγγράφου

9.3.1 Η πολιτική πρέπει να περιλαμβάνει τα ακόλουθα μεταδεδομένα και στοιχεία έκδοσης:

9.3.1.1 Τίτλο, αναγνωριστικό και επίπεδο ταξινόμησης

9.3.1.2 Ιδιοκτήτη πολιτικής και υπεύθυνο διαχείρισης εγγράφου

9.3.1.3 Ιστορικό αλλαγών και αιτιολόγηση επικαιροποιήσεων

9.3.1.4 Ημερομηνίες ανασκόπησης και επόμενης προγραμματισμένης επικαιροποίησης

9.3.1.5 Αναφορές διανομής και αρχείο αποδοχής

9.3.2 Το πρωτότυπο αντίγραφο πρέπει να τηρείται στο Αποθετήριο Εγγράφων του ISMS υπό έλεγχο εκδόσεων.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική πρέπει να ερμηνεύεται σε συνδυασμό με τις ακόλουθες:

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τις βασικές προσδοκίες συμπεριφοράς και τη δέσμευση της ανώτατης διοίκησης για την αποδεκτή χρήση.

10.1.2 P4 – Πολιτική Ελέγχου Πρόσβασης: Καθορίζει τις άδειες και τα δικαιώματα που συνδέονται με χρήστες, συστήματα και πρόσβαση σε δεδομένα, επιβάλλοντας άμεσα τα όρια αποδεκτής χρήσης.

10.1.3 P6 – Πολιτική Διαχείρισης Κινδύνων: Αντιμετωπίζει κινδύνους που σχετίζονται με τη συμπεριφορά και υποστηρίζει δραστηριότητες παρακολούθησης και αντιμετώπισης που συνδέονται με απειλές από ενέργειες χρηστών.

10.1.4 P7 – Πολιτική Ένταξης και Αποχώρησης: Διασφαλίζει ότι οι όροι αποδεκτής χρήσης αναγνωρίζονται κατά την ένταξη και ανακαλούνται κατά την αποχώρηση.

10.1.5 P9 – Πολιτική Απομακρυσμένης Εργασίας: Επεκτείνει τις διατάξεις αποδεκτής χρήσης σε περιβάλλοντα απομακρυσμένης και υβριδικής εργασίας.

10.2 Οι συναφείς αυτές πολιτικές συγκροτούν πολυεπίπεδο μοντέλο άμυνας για τη συμπεριφορική, τεχνική και συμβατική διακυβέρνηση.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα Πολιτική Αποδεκτής Χρήσης (AUP) ευθυγραμμίζεται με διεθνώς αναγνωρισμένα πρότυπα και νομικά πλαίσια, ώστε να διασφαλίζονται εφαρμόσιμοι, ελέγξιμοι και βασισμένοι στον κίνδυνο έλεγχοι συμπεριφοράς σε κάθε χρήση ψηφιακών και φυσικών πληροφοριακών συστημάτων.

11.2 ISO/IEC 27001:2022

11.2.1 Ρήτρα 5.10 – Αποδεκτή Χρήση Πληροφοριών και Άλλων Συναφών Περιουσιακών Στοιχείων: Η παρούσα πολιτική ικανοποιεί άμεσα την απαίτηση καθορισμού, γνωστοποίησης και εφαρμογής κανόνων που διέπουν την ορθή χρήση των πόρων ΤΠ.

11.2.2 Παράρτημα Α, Έλεγχος 6.1 – Ευθύνη για την Ασφάλεια Πληροφοριών: Αναθέτει σαφείς ευθύνες για τη συμπεριφορά των χρηστών και την εποπτεία της συμμόρφωσης.

11.2.3 Παράρτημα Α, Έλεγχος 6.2 – Ευαισθητοποίηση, Εκπαίδευση και Κατάρτιση για την Ασφάλεια Πληροφοριών: Οι διαδικασίες εκπαίδευσης και αποδοχής της πολιτικής αποτελούν μέρος της εφαρμογής της AUP.

11.2.4 Παράρτημα Α, Έλεγχος 8.1 – Συσκευές Τερματικών Σημείων Χρηστών και 8.12 – Πρόληψη Απώλειας Δεδομένων: Αντιμετωπίζει την αποδεκτή συμπεριφορά στις συσκευές χρηστών και διέπει δραστηριότητες που θα μπορούσαν να οδηγήσουν σε έκθεση ή διαρροή δεδομένων.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (Έλεγχος Πρόσβασης για Κινητές Συσκευές) και AC-20 (Χρήση Εξωτερικών Πληροφοριακών Συστημάτων): Η παρούσα πολιτική καθορίζει τις υποχρεώσεις και τους περιορισμούς των χρηστών για BYOD και πρόσβαση σε συστήματα τρίτων.

11.3.2 PL-4 (Κανόνες Συμπεριφοράς): Παρέχει λεπτομερείς απαιτήσεις αποδεκτής χρήσης που είναι συνεπείς με την παρούσα πολιτική.

11.3.3 AT-2 (Εκπαίδευση Ευαισθητοποίησης για την Ασφάλεια): Υποστηρίζεται μέσω εκπαίδευσης χρηστών και τεκμηριωμένης αποδοχής της πολιτικής.

11.3.4 AU-2 (Συμβάντα Ελέγχου) και AU-12 (Παραγωγή Αρχείων Ελέγχου): Η εφαρμογή βασίζεται στην παρακολούθηση ενεργειών χρηστών και στην ειδοποίηση για παραβιάσεις.

11.4 ΓΚΠΔ της ΕΕ (2016/679):

11.4.1 Άρθρο 5(1)(f): Επιβάλλει την ασφάλεια και την ακεραιότητα των δεδομένων προσωπικού χαρακτήρα. Η παρούσα πολιτική μετριάζει κινδύνους που εισάγονται από ανθρώπινη συμπεριφορά και μη εξουσιοδοτημένη χρήση.

11.4.2 Άρθρο 32: Απαιτεί τεχνικά και οργανωτικά μέτρα, όπως έλεγχοι συμπεριφοράς και περιορισμοί χρήσης, για την προστασία δεδομένων προσωπικού χαρακτήρα.

11.4.3 Αιτιολογική σκέψη 39: Αναδεικνύει την ανάγκη να διασφαλίζεται ότι μόνο εξουσιοδοτημένα άτομα έχουν την απολύτως αναγκαία πρόσβαση και νόμιμη χρήση των δεδομένων.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555):

11.5.1 Άρθρο 21(2)(a–d): Απαιτεί επιχειρησιακές πολιτικές και εκπαίδευση για ασφαλή χρήση συστημάτων, τις οποίες η παρούσα AUP παρέχει μέσω του καθορισμού συμπεριφοράς, της παρακολούθησης και των διαδικασιών εφαρμογής.

11.6 Κανονισμός DORA της ΕΕ (2022/2554):

11.6.1 Άρθρο 5: Η παρούσα πολιτική υποστηρίζει το πλαίσιο διαχείρισης κινδύνων ΤΠΕ, καθορίζοντας κανόνες για την αλληλεπίδραση ανθρώπου-συστήματος και ελαχιστοποιώντας την έκθεση σε κυβερνοκίνδυνο που βασίζεται στη συμπεριφορά.

11.7 COBIT 2019:

11.7.1 APO07 – Διαχειριζόμενο Ανθρώπινο Δυναμικό: Επιβάλλει ευθύνες χρηστών και ευαισθητοποίηση σε όλο τον κύκλο ζωής του εργαζομένου.

11.7.2 BAI05 – Διαχειριζόμενη Οργανωσιακή Αλλαγή: Ενσωματώνει τη διακυβέρνηση αποδεκτής χρήσης στις διαδικασίες αλλαγής που επηρεάζουν τη συμπεριφορά των χρηστών.

11.7.3 DSS05 – Διαχειριζόμενες Υπηρεσίες Ασφάλειας: Υποστηρίζει την παρακολούθηση δραστηριοτήτων χρηστών, τις ειδοποιήσεις συμπεριφοράς και τους αυτοματοποιημένους μηχανισμούς απόκρισης.

11.7.4 MEA01 – Παρακολούθηση, Αξιολόγηση και Εκτίμηση Απόδοσης και Συμμόρφωσης: Η πολιτική καθορίζει μετρικές και μηχανισμούς για την επικύρωση της συμμόρφωσης των χρηστών με τις προσδοκίες συμπεριφοράς.