					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P03S					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	Σχετίζεται με το συνολικό πλαίσιο και την εφαρμογή της πολιτικής
ISO/IEC 27002:2022	5.10, 5.11, 5	Παρέχει κατευθυντήριες οδηγίες για τις απαιτήσεις και τις δικλίδες αποδεκτής χρήσης
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Καλύπτει τη χρήση συστημάτων/συσκευών, την παρακολούθηση και την εκπαίδευση των χρηστών
ΓΚΠΔ	Άρθρα 5(1)(f), 32	Ακεραιότητα/εμπιστευτικότητα δεδομένων και μέτρα ασφάλειας
Οδηγία NIS2	Άρθρο 21(2)(b)	Επιβάλλει κατάλληλες πολιτικές ασφάλειας/αποδεκτής χρήσης
Κανονισμός DORA	Άρθρο 9	Πολιτική διαχείρισης κινδύνων ΤΠΕ, δικλίδες και εφαρμογή
COBIT 2019	DSS05, BAI08	Υπηρεσίες ασφάλειας και διαχείριση γνώσης

1. Σκοπός

1.1. Η παρούσα πολιτική καθορίζει την αποδεκτή, υπεύθυνη και ασφαλή χρήση των συστημάτων, συσκευών, της πρόσβασης στο διαδίκτυο, του ηλεκτρονικού ταχυδρομείου, των υπηρεσιών υπολογιστικού νέφους και κάθε προσωπικής συσκευής που χρησιμοποιείται για επιχειρησιακούς σκοπούς και παρέχεται ή εγκρίνεται από την εταιρεία.

1.2. Διασφαλίζει ότι τα εμπλεκόμενα πρόσωπα κατανοούν τις υποχρεώσεις τους κατά τη χρήση των πληροφοριακών πόρων του οργανισμού, με στόχο την προστασία της ακεραιότητας των δεδομένων, της ιδιωτικότητας και της επιχειρησιακής συνέχειας.

1.3. Η παρούσα πολιτική υποστηρίζει τη συμμόρφωση με το ISO/IEC 27001:2022, θεσπίζοντας σαφή πρότυπα συμπεριφοράς των χρηστών, ευθυγραμμισμένα με νομικές, συμβατικές και κανονιστικές απαιτήσεις.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε όλα τα πρόσωπα που αποκτούν πρόσβαση, διαχειρίζονται ή αλληλεπιδρούν με τα συστήματα ή τα δεδομένα της εταιρείας, συμπεριλαμβανομένων των εξής:

2.1.1. Εργαζομένων και αναδόχων

2.1.2. Προσωρινά απασχολούμενων ή ασκουμένων

2.1.3. Εξωτερικών παρόχων υπηρεσιών πληροφορικής

2.2. Καλύπτει:

2.2.1. Υπολογιστές, τηλέφωνα και ταμπλέτες που ανήκουν στην εταιρεία

2.2.2. Προσωπικές συσκευές εγκεκριμένες για επιχειρησιακή χρήση (BYOD)

2.2.3. Δίκτυα της εταιρείας, πλατφόρμες υπολογιστικού νέφους και υπηρεσίες λογισμικού

2.2.4. Πρόσβαση στο διαδίκτυο, συστήματα ηλεκτρονικού ταχυδρομείου, κοινόχρηστους αποθηκευτικούς χώρους και επιχειρησιακές εφαρμογές

2.3. Η παρούσα πολιτική εφαρμόζεται σε όλα τα περιβάλλοντα εργασίας — στις εγκαταστάσεις, εξ αποστάσεως ή υβριδικά — και σε όλες τις ώρες λειτουργίας.

3. Στόχοι

3.1. Να καθορίζει τι συνιστά αποδεκτή και μη αποδεκτή χρήση των συστημάτων ΤΠ.

3.1.1. Να μειώνει τους κινδύνους ασφάλειας που προκύπτουν από κακή χρήση, μη εξουσιοδοτημένη πρόσβαση ή εισαγωγή κακόβουλου λογισμικού.

3.1.2. Να προστατεύει τα επιχειρησιακά δεδομένα, τις πληροφορίες πελατών και τη φήμη της εταιρείας.

3.1.3. Να καθορίζει κανόνες που επιδέχονται εφαρμογή και να ενισχύει τη λογοδοσία όλων των χρηστών.

3.1.4. Να υποστηρίζει την παρακολούθηση και τη συμμόρφωση, ώστε οι παραβιάσεις να εντοπίζονται έγκαιρα και να λαμβάνονται διορθωτικά μέτρα.

4. Ρόλοι και αρμοδιότητες

4.1. Γενικός Διευθυντής

4.1.1. Εγκρίνει την παρούσα πολιτική και διασφαλίζει ότι διατίθενται οι απαιτούμενοι πόροι και η αναγκαία εξουσιοδότηση για την εφαρμογή της.

4.1.2. Ανασκοπεί και εγκρίνει τυχόν εξαιρέσεις από την παρούσα πολιτική.

4.2. Υπεύθυνος Πληροφορικής ή Εξωτερικός Πάροχος Υπηρεσιών Πληροφορικής

4.2.1. Τηρεί καταλόγους εγκεκριμένου λογισμικού και υλικού.

4.2.2. Παραμετροποιεί τις συσκευές ώστε να εφαρμόζονται οι κανόνες αποδεκτής χρήσης (π.χ. φιλτράρισμα περιεχομένου, καταγραφή πρόσβασης).

4.2.3. Παρακολουθεί τη χρήση για τον εντοπισμό πιθανών παραβιάσεων και διερευνά περιστατικά.

4.2.4. Διασφαλίζει ότι οι προσωπικές συσκευές (BYOD) εγκρίνονται και είναι ασφαλείς όταν χρησιμοποιούνται για επιχειρησιακούς σκοπούς.

[... 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 Υπεύθυνο Πληροφορικής, με τελική έγκριση από τον Γενικό Διευθυντή, ώστε να παραμένει ευθυγραμμισμένη με τα πρότυπα χρήσης της τεχνολογίας, τους αναδυόμενους κινδύνους και τις υποχρεώσεις συμμόρφωσης.

9.2. Ενδιάμεσοι ενεργοποιητές ανασκόπησης

9.2.1. Ανασκοπήσεις πρέπει επίσης να διενεργούνται σε περίπτωση:

9.2.2. Νέων συστημάτων ή τεχνολογιών (π.χ. νέα υπηρεσία υπολογιστικού νέφους ή νέα πλατφόρμα τερματικών συσκευών)

9.2.3. Σημαντικών παραβιάσεων της πολιτικής

9.2.4. Επικαιροποιημένων νόμων ή συμβατικών όρων που επηρεάζουν τη χρήση ΤΠ

9.3. Τεκμηρίωση αλλαγών

9.3.1. Όλες οι επικαιροποιήσεις πρέπει να καταγράφονται σε αρχείο εκδόσεων που περιλαμβάνει:

9.3.1.1. Αριθμό έκδοσης

9.3.1.2. Ημερομηνία ανασκόπησης

9.3.1.3. Σύνοψη αλλαγών

9.3.1.4. Αρχή έγκρισης

9.4. Κοινοποίηση της πολιτικής

9.4.1. Οι αναθεωρημένες εκδόσεις της παρούσας πολιτικής πρέπει να κοινοποιούνται σε όλους τους επηρεαζόμενους χρήστες. Οι εργαζόμενοι οφείλουν να επιβεβαιώνουν την παραλαβή και κατανόησή της στο πλαίσιο των υποχρεώσεών τους για ευαισθητοποίηση σε θέματα ασφάλειας.

10. Σχετικές πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική λειτουργεί σε συνδυασμό με άλλες πολιτικές SME, ώστε να διασφαλίζεται ολοκληρωμένη κάλυψη των αρμοδιοτήτων ασφάλειας:

10.1.1. P4S – Πολιτική Ελέγχου Πρόσβασης: Καθορίζει την τεχνική και διαδικαστική εφαρμογή της επιτρεπόμενης χρήσης και των περιορισμών λογαριασμών.

10.1.2. P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Παρέχει εκπαίδευση χρηστών σχετικά με τα όρια αποδεκτής χρήσης και τις υποχρεώσεις αναφοράς.

10.1.3. P9S – Πολιτική Εξ Αποστάσεως Εργασίας: Ρυθμίζει τη χρήση των συστημάτων της εταιρείας σε περιβάλλοντα εκτός εγκαταστάσεων ή κατ' οίκον εργασίας.

10.1.4. P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Επιβάλλει κανόνες χειρισμού δεδομένων προσωπικού χαρακτήρα που συνδέονται με την παρακολούθηση της αποδεκτής χρήσης και το BYOD.

10.1.5. P30S – Πολιτική Απόκρισης σε Περιστατικά: Διέπει τις διαδικασίες διερεύνησης και απόκρισης σε κακή χρήση ή παραβιάσεις των όρων αποδεκτής χρήσης.

11. Πρότυπα και πλαίσια αναφοράς

11.1. ISO/IEC 27001

11.1.1. Ρήτρα 5.10 – Απαιτεί από τους οργανισμούς να καθορίζουν και να εφαρμόζουν αποδεκτή χρήση των πληροφοριακών περιουσιακών στοιχείων.

11.2. ISO/IEC 27002

11.2.1. Δικλίδα 5.10 – Παρέχει κατευθυντήριες οδηγίες για την αποδεκτή χρήση συστημάτων, συμπεριλαμβανομένων επιτρεπόμενων και απαγορευμένων συμπεριφορών.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Καλύπτει τον έλεγχο της χρήσης συστημάτων, συμπεριλαμβανομένων προσωπικών συσκευών.

11.3.2. AC-20 – Απαιτεί εξουσιοδότηση και παρακολούθηση εξωτερικών συστημάτων.

11.3.3. AT-2 – Τονίζει την εκπαίδευση των χρηστών σε πρακτικές αποδεκτής χρήσης.

11.4. ΓΚΠΔ

11.4.1. Άρθρο 5(1)(f) – Απαιτεί ακεραιότητα και εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα, οι οποίες μπορεί να τεθούν σε κίνδυνο από κακή χρήση εκ μέρους των χρηστών.

11.4.2. Άρθρο 32 – Επιβάλλει την εφαρμογή τεχνικών και οργανωτικών μέτρων για την ασφάλεια συστημάτων και δεδομένων.

11.5. Οδηγία NIS2

11.5.1. Άρθρο 21(2)(b) – Απαιτεί κατάλληλες πολιτικές ασφάλειας, συμπεριλαμβανομένων κανόνων αποδεκτής χρήσης, για τον μετριασμό των κυβερνοαπειλών.

11.6. Κανονισμός DORA

11.6.1. Άρθρο 9 – Απαιτεί πολιτικές διαχείρισης κινδύνων ΤΠΕ, οι οποίες περιλαμβάνουν δικλίδες χρήσης και μηχανισμούς εφαρμογής.

11.7. COBIT 2019

11.7.1. DSS05 – Διαχείριση Υπηρεσιών Ασφάλειας: Τονίζει τον έλεγχο της συμπεριφοράς των χρηστών βάσει πολιτικών.

11.7.2. BAI08 – Διαχείριση Γνώσης: Καλύπτει την ευαισθητοποίηση σχετικά με τις αρμοδιότητες που απορρέουν από τις πολιτικές και την εκπαίδευση για την αποδεκτή χρήση.