					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P10					Τίτλος εγγράφου: **Πολιτική καθαρού γραφείου και καθαρής οθόνης**							
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**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Clause 6.1.3, Clause 8	Σχέδιο αντιμετώπισης κινδύνων, επιχειρησιακός σχεδιασμός και έλεγχος για ασφαλείς χώρους εργασίας
ISO/IEC 27002:2022	Control 7	Έλεγχοι συμπεριφοράς και περιβαλλοντικοί έλεγχοι για την προστασία αφύλακτων φυσικών πληροφοριών
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	Φυσική πρόσβαση, ασφάλεια εργολάβων, διάθεση μέσων, κλείδωμα συνόδου, έλεγχοι ρυθμίσεων και μηχανισμών αυθεντικοποίησης
ΓΚΠΔ της ΕΕ	Articles 5(1)(f), 32; Recital 39	Ακεραιότητα και εμπιστευτικότητα δεδομένων και φυσικές δικλίδες ασφαλείας για δεδομένα
Οδηγία NIS2 της ΕΕ	Articles 21(2)(d), 21(3)	Πολιτικές για φυσική ασφάλεια, συμπεριφορά χρηστών και πρόληψη διαρροής
Κανονισμός DORA της ΕΕ	Articles 5, 8, 9	Εσωτερική διακυβέρνηση ΤΠΕ και διαχείριση περιστατικών που περιλαμβάνει φυσική ασφάλεια
COBIT 2019	DSS01, DSS05, MEA	Διαχειριζόμενες λειτουργίες, υπηρεσίες ασφάλειας και παρακολούθηση συμμόρφωσης

1. Σκοπός

1.1 Η παρούσα πολιτική θεσπίζει υποχρεωτικούς ελέγχους για την προστασία ευαίσθητων πληροφοριών, απαιτώντας τον ασφαλή χειρισμό φυσικών εγγράφων, σταθμών εργασίας, οθονών και αφαιρούμενων μέσων τόσο σε περιβάλλον γραφείου όσο και σε κοινόχρηστους χώρους εργασίας.

1.2 Υποστηρίζει το Παράρτημα Α του ISO/IEC 27001, Έλεγχο 7.7, μέσω της εφαρμογής ελέγχων συμπεριφοράς και τεχνικών πρακτικών που μετριάζουν τον κίνδυνο μη εξουσιοδοτημένης γνωστοποίησης, κλοπής ή απώλειας δεδομένων λόγω αφύλακτων ή ορατών πληροφοριών.

1.3 Η παρούσα πολιτική ενισχύει τη φυσική ασφάλεια και την ασφάλεια πληροφοριών στην καθημερινή λειτουργία και υποστηρίζει τη συμμόρφωση με τις εφαρμοστέες νομικές, συμβατικές και κανονιστικές υποχρεώσεις.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλο το προσωπικό που εργάζεται ή αποκτά πρόσβαση σε φυσικούς χώρους εργασίας, συμπεριλαμβανομένων των εξής:

2.1.1 Μόνιμοι και προσωρινοί εργαζόμενοι

2.1.2 Εργολάβοι, σύμβουλοι, προμηθευτές και ασκούμενοι

2.1.3 Τρίτοι πάροχοι υπηρεσιών και επιτόπιοι επισκέπτες με πρόσβαση σε ευαίσθητες πληροφορίες

2.2 Οι απαιτήσεις εφαρμόζονται στα εξής:

2.2.1 Ατομικά γραφεία, διαχωρισμένους χώρους εργασίας και χώρους ανοικτής διάταξης

2.2.2 Αίθουσες συσκέψεων και κοινόχρηστους χώρους συνεργασίας

2.2.3 Σημεία εκτύπωσης, γραφεία υποδοχής και χώρους φωτοαντιγραφής

2.2.4 Χώρους όπου χρησιμοποιούνται απομακρυσμένοι σταθμοί εργασίας ή κοινόχρηστα περίπτερα

2.3 Η παρούσα πολιτική εφαρμόζεται επίσης σε προσωρινά ή υβριδικά περιβάλλοντα εργασίας (π.χ. hot-desking) και σε χώρους με πρόσβαση κοινού όπου υφίσταται κίνδυνος οπτικής υποκλοπής ή ύπαρξης αφύλακτων δεδομένων.

3. Στόχοι

3.1 Η αποτροπή μη εξουσιοδοτημένης πρόσβασης σε εμπιστευτικές, ευαίσθητες ή ρυθμιζόμενες πληροφορίες που παραμένουν εκτεθειμένες σε φυσική ή ψηφιακή μορφή.

3.2 Η προώθηση τυποποιημένης προσέγγισης στον κίνδυνο ασφάλειας σε όλα τα περιβάλλοντα εργασίας μέσω της χρήσης φυσικών δικλίδων ασφαλείας, της ρύθμισης παραμέτρων σταθμών εργασίας και της συμπεριφοράς των τελικών χρηστών.

3.3 Η μείωση του κινδύνου παραβιάσεων ιδιωτικότητας, απώλειας πνευματικής ιδιοκτησίας και εξαγωγής δεδομένων λόγω αμέλειας ή ελλιπούς εποπτείας.

3.4 Η ενσωμάτωση πρακτικών καθαρού γραφείου και καθαρής οθόνης στην οργανωσιακή κουλτούρα, με σκοπό την υποστήριξη της λειτουργικής πειθαρχίας, της δυνατότητας ελέγχου και της νομικής τεκμηρίωσης.

3.5 Η υποστήριξη της συμμόρφωσης με το ISO/IEC 27001, το Άρθρο 32 του ΓΚΠΔ, το Άρθρο 21 της Οδηγίας NIS2 της ΕΕ και άλλες απαιτήσεις φυσικής ασφάλειας που σχετίζονται με κρίσιμα ή προσωπικά δεδομένα.

4. Ρόλοι και αρμοδιότητες

4.1 Ανώτατη Διοίκηση

4.1.1 Εγκρίνει την παρούσα πολιτική και προάγει κουλτούρα ασφάλειας σε όλες τις επιχειρησιακές μονάδες.

4.1.2 Διαθέτει κατάλληλους πόρους για την εφαρμογή της πολιτικής, εκστρατείες ευαισθητοποίησης και μηχανισμούς φυσικού ελέγχου.

4.2 Επικεφαλής Ασφάλειας Πληροφοριών / Υπεύθυνος ΣΔΑΠ

4.2.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και διασφαλίζει την ευθυγράμμισή της με το ISO/IEC 27001:2022, τις απαιτήσεις ελέγχου και τις στρατηγικές αντιμετώπισης κινδύνων.

4.2.2 Αναπτύσσει προγράμματα ευαισθητοποίησης και ελέγχους ώστε να διασφαλίζεται η συνεπής εφαρμογή σε εγκαταστάσεις και σε υβριδικά περιβάλλοντα εργασίας.

4.2.3 Συντονίζεται με τις αρμόδιες λειτουργίες Εγκαταστάσεων και Πληροφορικής, ώστε να διασφαλίζεται η ύπαρξη κατάλληλων φυσικών δικλίδων ασφαλείας.

[... 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 Χρονοδιάγραμμα ανασκόπησης πολιτικής

9.1.1 Η παρούσα πολιτική ανασκοπείται:

9.1.1.1 Τουλάχιστον ετησίως

9.1.1.2 Μετά από οποιαδήποτε μη συμμόρφωση ελέγχου που σχετίζεται με έκθεση χώρου εργασίας ή οθόνης

9.1.1.3 Κατόπιν φυσικού ή περιβαλλοντικού περιστατικού (π.χ. κλοπή συσκευής, tailgating, επιτήρηση)

9.1.1.4 Με την εφαρμογή νέων διατάξεων γραφείου, πολιτικών εγκαταστάσεων ή μοντέλων χώρου εργασίας (π.χ. hot desking, απομακρυσμένοι κόμβοι)

9.2 Υπεύθυνοι ιδιοκτήτες

9.2.1 Ιδιοκτήτης της πολιτικής είναι ο Επικεφαλής Ασφάλειας Πληροφοριών ή ο ορισμένος Υπεύθυνος ΣΔΑΠ.

9.2.2 Η διαδικασία ανασκόπησης περιλαμβάνει:

9.2.2.1 Ομάδες Εγκαταστάσεων και Εταιρικής Ασφάλειας

9.2.2.2 Πληροφορική και Υποδομές για την εφαρμογή που σχετίζεται με συσκευές

9.2.2.3 Ανθρώπινο Δυναμικό και Νομικό Τμήμα για την εφαρμογή κανόνων συμπεριφοράς και την ευθυγράμμιση πειθαρχικών μέτρων

9.2.3 Όλες οι επικαιροποιήσεις της πολιτικής πρέπει να ελέγχονται ως προς την έκδοση, να εγκρίνονται από την Επιτροπή Καθοδήγησης ΣΔΑΠ και να αναδιανέμονται με εκ νέου επιβεβαίωση αποδοχής όπου απαιτείται.

9.3 Επικοινωνία αλλαγών

9.3.1 Οι χρήστες ενημερώνονται για ουσιώδεις επικαιροποιήσεις μέσω:

9.3.1.1 Του κέντρου πολιτικών ή της πύλης intranet

9.3.1.2 Στοχευμένων επικοινωνιών μέσω ηλεκτρονικού ταχυδρομείου

9.3.1.3 Επαναληπτικών ενημερώσεων κατά την ένταξη και τριμηνιαίων ενημερώσεων

9.3.1.4 Υποχρεωτικών προτροπών αποδοχής για κάθε νέα κρίσιμη ρήτρα εφαρμογής

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική ευθυγραμμίζεται και υποστηρίζει τα ακόλουθα:

10.1.1 P1 – Πολιτική Ασφάλειας Πληροφοριών: Καθορίζει τις προσδοκίες για τη συμπεριφορά των χρηστών και τη φυσική ασφάλεια που αποτελούν τη βάση της παρούσας πολιτικής.

10.1.2 P3 – Πολιτική Αποδεκτής Χρήσης: Καλύπτει τη λογοδοσία των χρηστών για την προστασία δεδομένων και συστημάτων, συμπεριλαμβανομένων των φυσικών περιβαλλόντων.

10.1.3 P6 – Πολιτική Διαχείρισης Κινδύνων: Ενσωματώνει τους κινδύνους φυσικών χώρων εργασίας ως μέρος της συνολικής ανάλυσης κινδύνων πληροφοριών σε επίπεδο επιχείρησης.

10.1.4 P12 – Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Υποστηρίζει την ιχνηλάτηση και τον ασφαλή χειρισμό συσκευών και μέσων που παραμένουν σε γραφεία.

10.1.5 P13 – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Διασυνδέεται με την εφαρμογή καθαρού γραφείου για φυσικά έγγραφα που φέρουν επισήμανση Εμπιστευτικό ή Εσωτερικό.

10.1.6 P14 – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Καθοδηγεί τις πρακτικές διατήρησης φυσικών εγγράφων, καταστροφής και χειρισμού κάδων.

10.1.7 P22 – Πολιτική Καταγραφής και Παρακολούθησης: Μπορεί να χρησιμοποιείται για την παρακολούθηση της κατάστασης κλειδώματος σταθμών εργασίας, του χρόνου αδράνειας ή ροών από κάμερες χώρων εργασίας, όπου αυτό επιτρέπεται.

10.2 Οι συναφείς αυτές πολιτικές θεμελιώνουν μια ολοκληρωμένη κουλτούρα ασφάλειας, συνδυάζοντας την ευαισθητοποίηση χρηστών, τις φυσικές δικλίδες ασφαλείας και τη λογοδοσία, ώστε να διασφαλίζονται ανθεκτικοί χώροι εργασίας.

11. Πρότυπα και πλαίσια αναφοράς

11.1 Η παρούσα πολιτική είναι ευθυγραμμισμένη με διεθνώς αναγνωρισμένα πρότυπα και νομικές απαιτήσεις που επιβάλλουν την προστασία ευαίσθητων πληροφοριών σε φυσικά περιβάλλοντα και μέσω της συμπεριφοράς των χρηστών.

11.2 ISO/IEC 27001

11.2.1 Clause 6.1.3 – Σχέδιο Αντιμετώπισης Κινδύνων: Υποστηρίζει την εφαρμογή ελέγχων για τον μετριασμό φυσικών και περιβαλλοντικών κινδύνων, συμπεριλαμβανομένων εκείνων που συνδέονται με τη συμπεριφορά χρηστών σε ανοικτούς χώρους εργασίας.

11.2.2 Clause 8.1 – Επιχειρησιακός σχεδιασμός και έλεγχος: Καθορίζει επιχειρησιακές δικλίδες ασφαλείας για τη διαχείριση ασφαλών χώρων εργασίας και της χρήσης εξοπλισμού.

11.3 ISO/IEC 27002:2022 – Control 7

11.3.1 Ο έλεγχος αυτός απαιτεί ελέγχους συμπεριφοράς και περιβαλλοντικής προστασίας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες μέσω αφύλακτων μέσων, οθονών ή εκτυπωμένων υλικών. Η πολιτική εφαρμόζει πρακτικές υγιεινής φυσικού χώρου εργασίας, χρήση κλειδώματος οθόνης και ασφαλή διάθεση ευαίσθητων εγγράφων.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (Physical Access Authorizations): Συνδέεται με περιορισμούς χώρων εργασίας και την επιβολή κλειδωμένης αποθήκευσης σε περιβάλλοντα υψηλού κινδύνου.

11.4.2 PS-7 (External Personnel Security): Εφαρμόζεται μέσω απαιτήσεων καθαρού γραφείου και καθαρής οθόνης που επεκτείνονται σε εργολάβους και χρήστες τρίτων μερών.

11.4.3 MP-6 (Media Sanitization) και AC-11 (Session Lock): Υλοποιούνται μέσω διαδικασιών ασφαλούς διάθεσης και υποχρεωτικών χρονόμετρων κλειδώματος οθόνης.

11.4.4 CM-6 (Configuration Settings) και IA-5 (Authenticator Management): Υποστηρίζουν την τεχνική εφαρμογή του κλειδώματος οθόνης και του ελέγχου συνόδου σε τερματικά.

11.5 ΓΚΠΔ της ΕΕ (2016/679)

11.5.1 Άρθρο 5(1)(f): Επιβάλλει ακεραιότητα και εμπιστευτικότητα των προσωπικών δεδομένων, συμπεριλαμβανομένης της προστασίας από φυσική έκθεση ή θέαση από μη εξουσιοδοτημένα πρόσωπα.

11.5.2 Άρθρο 32 – Ασφάλεια επεξεργασίας: Απαιτεί κατάλληλα τεχνικά και οργανωτικά μέτρα και φυσικά μέτρα για την προστασία προσωπικών δεδομένων από τυχαία ή παράνομη καταστροφή, απώλεια ή μη εξουσιοδοτημένη γνωστοποίηση — κάτι που επιτυγχάνεται μέσω ελέγχων γραφείου και οθόνης.

11.5.3 Αιτιολογική σκέψη 39: Απαιτεί τον περιορισμό της πρόσβασης σε προσωπικά δεδομένα μόνο σε εξουσιοδοτημένα άτομα — αυτό περιλαμβάνει και την ασφάλισή τους σε φυσική μορφή όταν παραμένουν χωρίς επιτήρηση.

11.6 Οδηγία NIS2 της ΕΕ (2022/2555)

11.6.1 Άρθρο 21(2)(d): Απαιτεί πολιτικές και διαδικασίες σχετικές με τη φυσική και περιβαλλοντική ασφάλεια, συμπεριλαμβανομένων μέτρων προστασίας της ασφάλειας πληροφοριών σε επίπεδο χώρου εργασίας.

11.6.2 Άρθρο 21(3): Ενθαρρύνει κουλτούρα ασφάλειας που ενσωματώνει ορθή συμπεριφορά χρηστών, ευαισθητοποίηση και πρόληψη ακούσιων διαρροών δεδομένων — κάτι που υποστηρίζεται από τους ελέγχους συμπεριφοράς της παρούσας πολιτικής.

11.7 Κανονισμός DORA της ΕΕ (2022/2554)

11.7.1 Άρθρο 5 – Εσωτερική διακυβέρνηση και έλεγχος: Απαιτεί όλοι οι κίνδυνοι που σχετίζονται με τις ΤΠΕ, συμπεριλαμβανομένων ανθρώπινων και περιβαλλοντικών απειλών, να διέπονται από εφαρμοστέες πολιτικές.

11.7.2 Άρθρο 8 – Διαχείριση κινδύνων ΤΠΕ: Επιβάλλει δικλίδες ασφαλείας τόσο σε ψηφιακά όσο και σε φυσικά πλαίσια, διασφαλίζοντας ότι οι απομακρυσμένοι χρήστες, οι χρήστες υποκαταστημάτων και οι χρήστες εντός των εγκαταστάσεων δεν δημιουργούν μη διαχειριζόμενη έκθεση.

11.7.3 Άρθρο 9 – Διαχείριση περιστατικών: Απαιτεί περιβαλλοντικές ή συμπεριφορικές παραλείψεις που οδηγούν σε έκθεση δεδομένων να καταγράφονται, να ταξινομούνται και να αντιμετωπίζονται με κατάλληλες διορθωτικές ενέργειες.

11.8 COBIT 2019

11.8.1 DSS01 – Managed Operations: Διασφαλίζει λειτουργική πειθαρχία στην προστασία φυσικών χώρων εργασίας και συστημάτων μέσω επαναλαμβανόμενων ελέγχων.

11.8.2 DSS05 – Managed Security Services: Υποστηρίζει την προστασία δεδομένων, συσκευών και σημείων πρόσβασης μέσω εφαρμογής βασισμένης στη συμπεριφορά, όπως οι πρακτικές καθαρού γραφείου.

11.8.3 MEA03 – Monitor, Evaluate, and Assess Compliance: Ενθαρρύνει τον έλεγχο φυσικών δικλίδων ασφαλείας και της υιοθέτησης πολιτικών στις καθημερινές επιχειρησιακές πρακτικές.