					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P10S					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	Ρήτρες 7.2, 8	
ISO/IEC 27002:2022	Έλεγχος 7	
NIST SP 800-53 Rev.5	PE-2, AC-11	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(d)	
Κανονισμός DORA της ΕΕ	Άρθρο 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
ΓΚΠΔ της ΕΕ	Άρθρο 32	

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει δεσμευτικές απαιτήσεις για τη διατήρηση ασφαλούς περιβάλλοντος εργασίας, διασφαλίζοντας ότι τα γραφεία, οι σταθμοί εργασίας και οι οθόνες δεν εμφανίζουν ορατές εμπιστευτικές πληροφορίες όταν παραμένουν χωρίς επιτήρηση.

1.2 Κύριος σκοπός της είναι η πρόληψη μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητες πληροφορίες μέσω εκτυπώσεων που παραμένουν αφύλακτες, μη κλειδωμένων οθονών ή αφύλακτων αφαιρούμενων μέσων, τόσο σε φυσικούς χώρους γραφείου όσο και σε χώρους τηλεργασίας.

1.3 Οι πρακτικές καθαρού γραφείου και καθαρής οθόνης που ορίζονται στην παρούσα πολιτική ενισχύουν την ικανότητα του οργανισμού να ανταποκρίνεται στις απαιτήσεις πιστοποίησης ISO/IEC 27001, μειώνοντας αποτρέψιμους κινδύνους έκθεσης. Οι πρακτικές αυτές τεκμηριώνουν επίσης προς πελάτες, συνεργάτες και ελεγκτές ότι ο οργανισμός αντιμετωπίζει με τη δέουσα σοβαρότητα την ασφάλεια πληροφοριών, ακόμη και σε περιβάλλοντα με περιορισμένους πόρους.

1.4 Η παρούσα πολιτική υποστηρίζει κουλτούρα λογοδοσίας και ευαισθητοποίησης, διασφαλίζοντας ότι όλο το προσωπικό — ανεξαρτήτως ρόλου ή τεχνικής εξειδίκευσης — κατανοεί την ευθύνη του για την προστασία πληροφοριών της εταιρείας και των πελατών από οπτική έκθεση, κλοπή ή απώλεια.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλους τους εργαζομένους, αναδόχους, ασκούμενους και το προσωρινό προσωπικό που χρησιμοποιούν σταθμούς εργασίας, γραφεία ή φορητές συσκευές που ανήκουν στην εταιρεία ή τους έχουν ανατεθεί

2.1.2 Όλους τους φυσικούς χώρους που χρησιμοποιούνται για επιχειρησιακή δραστηριότητα, συμπεριλαμβανομένων αποκλειστικών γραφείων, συνεργατικών χώρων εργασίας και απομακρυσμένων/οικιακών χώρων εργασίας

2.1.3 Όλες τις ψηφιακές συσκευές με δυνατότητα απεικόνισης, συμπεριλαμβανομένων επιτραπέζιων υπολογιστών, φορητών υπολογιστών, tablet και εξωτερικών οθονών που χρησιμοποιούνται για επιχειρησιακούς σκοπούς

2.2 Η πολιτική καλύπτει κάθε φυσικό ή ψηφιακό περιουσιακό στοιχείο που μπορεί να εμφανίζει, να περιέχει ή να μεταδίδει ευαίσθητες πληροφορίες, συμπεριλαμβανομένων:

2.2.1 Έντυπων αρχείων ή χειρόγραφων σημειώσεων

2.2.2 Μονάδων USB, CD και εξωτερικών σκληρών δίσκων

2.2.3 Κινητών τηλεφώνων που χρησιμοποιούνται για επιχειρησιακή ανταλλαγή μηνυμάτων ή ηλεκτρονικό ταχυδρομείο

2.2.4 Οθονών υπολογιστών και προβολέων που συνδέονται με συστήματα εργασίας

2.3 Η παρούσα πολιτική εξακολουθεί να εφαρμόζεται εκτός κανονικού ωραρίου εργασίας και κατά τη διάρκεια μη συνήθων λειτουργιών, όπως συντήρηση εκτός ωραρίου ή εργασία απόκρισης σε περιστατικά.

3. Στόχοι

3.1 Η εφαρμογή πρακτικών και συνεπών ελέγχων, ώστε να διασφαλίζεται ότι καμία ευαίσθητη πληροφορία δεν παραμένει εκτεθειμένη σε γραφεία, οθόνες ή κοινόχρηστους χώρους.

3.2 Η ελαχιστοποίηση του κινδύνου μη εξουσιοδοτημένης πρόσβασης, τόσο από εσωτερικές πηγές, όπως ακούσια πρόσβαση από άλλους εργαζομένους, όσο και από εξωτερικές απειλές, όπως επισκέπτες, προσωπικό καθαριότητας ή ανάδοχοι.

3.3 Η υποστήριξη ελέγχων λογικής και φυσικής πρόσβασης, απαιτώντας από το προσωπικό να προστατεύει ενεργά το υλικό εργασίας και να κλειδώνει τους υπολογιστές όταν δεν είναι παρόν.

3.4 Η ενίσχυση της ευαισθητοποίησης του προσωπικού σχετικά με ασφαλείς πρακτικές εργασίας και η παροχή απλών, δεσμευτικών κανόνων που εφαρμόζονται στην καθημερινή λειτουργία, ανεξαρτήτως τοποθεσίας εργασίας.

3.5 Η διασφάλιση ευθυγράμμισης με το Παράρτημα A του ISO/IEC 27001, έλεγχο 7.7, και με τις οδηγίες εφαρμογής του ISO/IEC 27002 για τις απαιτήσεις καθαρού γραφείου και καθαρής οθόνης.

3.6 Η διασφάλιση ότι ο οργανισμός μπορεί να αποδεικνύει δέουσα επιμέλεια και ετοιμότητα για έλεγχο χωρίς να απαιτείται υποδομή εταιρικής κλίμακας.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Έχει την ευθύνη της παρούσας πολιτικής και διασφαλίζει ότι κοινοποιείται δεόντως, γίνεται κατανοητή και τηρείται από όλους τους εργαζομένους και αναδόχους.

4.1.2 Είναι υπεύθυνος για την έγκριση τυχόν εξαιρέσεων, την απόκριση σε παραβιάσεις και την εποπτεία της εκπαίδευσης που σχετίζεται με ασφαλείς πρακτικές εργασίας.

4.1.3 Οφείλει να διενεργεί ή να αναθέτει τακτικούς ελέγχους, τουλάχιστον ανά τρίμηνο, για να επιβεβαιώνει ότι οι φυσικοί και ψηφιακοί χώροι εργασίας πληρούν τις απαιτήσεις της πολιτικής.

4.2 Ορισμένο μέλος του προσωπικού (εφόσον έχει οριστεί)

4.2.1 Μπορεί να του ανατεθεί η ευθύνη για την εφαρμογή τεχνικών ρυθμίσεων, όπως ρυθμίσεις χρονικού ορίου οθόνης, ή για τη διάθεση φυσικών μέσων αποθήκευσης, όπως συρτάρια με κλειδαριά.

4.2.2 Υποστηρίζει τον GM με την αναφορά μη συμμορφώσεων, τη διαχείριση υπενθυμίσεων ασφάλειας του χώρου εργασίας και την παρακολούθηση ενεργειών αποκατάστασης όταν εντοπίζονται ζητήματα.

4.2.3 Συμβάλλει ώστε όλοι οι εργαζόμενοι να έχουν πρόσβαση, όπου είναι εφικτό, σε κατάλληλους μηχανισμούς κλειδώματος ή ασφαλείς χώρους αποθήκευσης.

[... 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 Ο GM οφείλει να ανασκοπεί την παρούσα πολιτική τουλάχιστον μία φορά ετησίως και μετά από οποιοδήποτε από τα ακόλουθα γεγονότα:

9.1.1 Εισαγωγή νέων χώρων γραφείου, συσκευών ή κοινόχρηστων συστημάτων

9.1.2 Αλλαγές στις εφαρμοστέες νομικές απαιτήσεις ή απαιτήσεις πιστοποίησης

9.1.3 Ευρήματα από ελέγχους, εκτιμήσεις κινδύνων ή περιστατικά ασφάλειας

9.2 Ενδιάμεσες επικαιροποιήσεις πρέπει να κοινοποιούνται σε όλους τους εργαζομένους μέσω ηλεκτρονικού ταχυδρομείου, με υποχρεωτική επιβεβαίωση παραλαβής.

9.3 Οι προηγούμενες εκδόσεις της παρούσας πολιτικής πρέπει να αποθηκεύονται με ασφαλή τρόπο και να είναι διαθέσιμες για έλεγχο, ώστε να αποδεικνύεται η συνεχής ευθυγράμμιση με το ISO/IEC 27001 και τα συναφή πλαίσια.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Αποσαφηνίζει την αρμοδιότητα του GM να εφαρμόζει την πολιτική και να διενεργεί ελέγχους σχετικά με τη συμπεριφορά σε φυσικούς και ψηφιακούς χώρους εργασίας.

10.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Υποστηρίζει την τεχνική εφαρμογή του κλειδώματος οθόνης και των ασφαλών πρακτικών σύνδεσης σε σταθμούς εργασίας.

10.3 P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Ενισχύει την εκπαίδευση συμπεριφοράς που απαιτείται για τη συμμόρφωση με την πολιτική.

10.4 P17S – Πολιτική προστασίας δεδομένων και ιδιωτικότητας: Καθορίζει τις υποχρεώσεις για τον χειρισμό και την προστασία δεδομένων προσωπικού χαρακτήρα και ευαίσθητων δεδομένων σε συμμόρφωση με τον ΓΚΠΔ της ΕΕ.

10.5 P30S – Πολιτική αντιμετώπισης περιστατικών: Παρέχει το πλαίσιο κλιμάκωσης και απόκρισης όταν μια παραβίαση οδηγεί σε έκθεση δεδομένων ή συμβάν ασφάλειας.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 7.2: Απαιτεί όλο το προσωπικό να γνωρίζει τις αρμοδιότητές του για την ασφάλεια, συμπεριλαμβανομένης της φυσικής προστασίας.

11.1.2 Ρήτρα 8.1: Οι επιχειρησιακοί έλεγχοι πρέπει να διασφαλίζουν κατάλληλες φυσικές και λογικές δικλίδες ασφαλείας.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 7.7: Παρέχει αναλυτική καθοδήγηση για την καθιέρωση, κοινοποίηση και εφαρμογή απαιτήσεων καθαρού γραφείου και καθαρής οθόνης.

11.3 NIST SP 800-53 Rev.5

11.3.1 PE-2: Καθορίζει τις απαιτήσεις ελέγχου φυσικής πρόσβασης, συμπεριλαμβανομένης της συμπεριφοράς του προσωπικού σε ασφαλή περιβάλλοντα.

11.3.2 AC-11: Επιβάλλει λειτουργία κλειδώματος συνεδρίας για σταθμούς εργασίας, ώστε να αποτρέπεται μη εξουσιοδοτημένη θέαση ή αλληλεπίδραση.

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Άρθρο 32: Απαιτεί από τους οργανισμούς να προστατεύουν τα δεδομένα προσωπικού χαρακτήρα με φυσικές και τεχνικές δικλίδες ασφαλείας, συμπεριλαμβανομένων των σταθμών εργασίας και των εγγράφων.

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Άρθρο 21(2)(d): Απαιτεί από τους οργανισμούς να εφαρμόζουν πολιτικές φυσικής και λογικής πρόσβασης βάσει κινδύνου.

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Άρθρο 9(2)(f): Επιβάλλει πολιτικές ασφάλειας ΤΠΕ, συμπεριλαμβανομένης της ασφαλούς υγιεινής του χώρου εργασίας, για τους φορείς του χρηματοπιστωτικού τομέα και τις εφοδιαστικές τους αλυσίδες.

11.7 COBIT 2019

11.7.1 DSS01.06: Απαιτεί πρακτικές προστασίας περιουσιακών στοιχείων, συμπεριλαμβανομένων φυσικών ελέγχων σε χώρους εργασίας και μέσα.

11.7.2 DSS05.02: Υποστηρίζει την εφαρμογή πρακτικών ασφάλειας τελικών χρηστών σε όλα τα λειτουργικά περιβάλλοντα.