					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: PII18					Τίτλος εγγράφου: **Πολιτική Παρακολούθησης, Ελέγχου και Βελτίωσης του PIMS**							
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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Μέτρηση στόχων ιδιωτικότητας
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Τεκμηριωμένες πληροφορίες παρακολούθησης, ελέγχου και βελτίωσης
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Παρακολούθηση επιχειρησιακού σχεδιασμού και ελέγχου
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Εσωτερικός έλεγχος
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Ανασκόπηση της Διοίκησης
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Συνεχής βελτίωση
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Μη συμμόρφωση και διορθωτικά μέτρα
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Αρχεία επεξεργασίας υπευθύνου επεξεργασίας που χρησιμοποιούνται για έλεγχο
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Συμφωνία εκτελούντος την επεξεργασία και τεκμήρια συνεργασίας σε ελέγχους
GDPR	Article 5(2)	Controller	Supporting	Τεκμήρια λογοδοσίας
GDPR	Article 24	Controller	Supporting	Μέτρα υπευθύνου επεξεργασίας και ανασκόπηση αποτελεσματικότητας
GDPR	Article 28	Both	Supporting	Διακυβέρνηση ελέγχου και συνεργασίας

				εκτελούντος την επεξεργασία
GDPR	Article 30	Both	Supporting	Αρχεία επεξεργασίας που χρησιμοποιούνται για έλεγχο
GDPR	Article 32	Both	Supporting	Δοκιμή και αξιολόγηση μέτρων ασφάλειας
GDPR	Article 39	Conditional	Supporting	Παρακολούθηση από DPO και συμβουλές ελέγχου, όπου εφαρμόζεται
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Συμμόρφωση, έλεγχος και ανεξάρτητη εποπτεία ιδιωτικότητας
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Ανασκόπηση προστασίας PII και έλεγχοι συμμόρφωσης
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Παρακολούθηση και αξιολόγηση ασφάλειας πληροφοριών
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Υποστήριξη εσωτερικού ελέγχου ISMS
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Υποστήριξη ανασκόπησης της Διοίκησης του ISMS
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Υποστήριξη συνεχούς βελτίωσης του ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Υποστήριξη μη συμμόρφωσης και διορθωτικών μέτρων του ISMS
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Ανεξάρτητη ανασκόπηση της ασφάλειας πληροφοριών
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Ανασκόπηση συμμόρφωσης πολιτικών και προτύπων

ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Αρχές, πρόγραμμα, διεξαγωγή και επάρκεια ελέγχων συστήματος διαχείρισης

1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική καθορίζει τις απαιτήσεις του οργανισμού για την παρακολούθηση, τη μέτρηση, την ανάλυση, την αξιολόγηση, τον εσωτερικό έλεγχο, την ανασκόπηση της Διοίκησης, τη διαχείριση μη συμμορφώσεων, τα διορθωτικά μέτρα και τη συνεχή βελτίωση του PIMS.

1.2 Η παρούσα πολιτική εφαρμόζεται στα ακόλουθα:

1.2.1 όλες τις διεργασίες, ελέγχους, πολιτικές, μητρώα, αντικείμενα τεκμηρίων, συστήματα, προμηθευτές, εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας και ρυθμίσεις κοινοχρησίας δεδομένων εντός του πεδίου εφαρμογής του PIMS·

1.2.2 τα πλαίσια του οργανισμού ως υπευθύνου επεξεργασίας, από κοινού υπευθύνου επεξεργασίας, εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας·

1.2.3 την ενοποιημένη παρακολούθηση της απόδοσης του PIMS, των στόχων ιδιωτικότητας, της κατάστασης υλοποίησης των ελέγχων, των ευρημάτων ελέγχου, των μη συμμορφώσεων, των διορθωτικών ενεργειών, των ενεργειών ανασκόπησης της Διοίκησης και των ενεργειών βελτίωσης·

1.2.4 τα τεκμήρια που τηρούνται στο REG12 και τα υποστηρικτικά τεκμήρια πηγής που τηρούνται στα REG01 έως REG11.

1.3 Η παρούσα πολιτική δεν αντικαθιστά τις απαιτήσεις επιχειρησιακής παρακολούθησης που ορίζονται σε άλλες πολιτικές PIMS. Καθορίζει τον ενοποιημένο κύκλο αξιολόγησης απόδοσης, ελέγχου, ανασκόπησης και βελτίωσης για το PIMS.

1.4 Για τους σκοπούς της παρούσας πολιτικής, μείζων μη συμμόρφωση PIMS σημαίνει αστοχία που επηρεάζει ουσιωδώς το πεδίο εφαρμογής του PIMS, τους στόχους ιδιωτικότητας, τη λογοδοσία επεξεργασίας PII, την αντιμετώπιση κινδύνου ιδιωτικότητας, τα δικαιώματα υποκειμένων των δεδομένων προσωπικού χαρακτήρα, την ασφάλεια της επεξεργασίας, τη διακυβέρνηση εκτελούντων την επεξεργασία ή υπεργολάβων επεξεργασίας, την ετοιμότητα για παραβίαση, την ακεραιότητα τεκμηριωμένων τεκμηρίων, το πεδίο πιστοποίησης ή την επαναλαμβανόμενη αστοχία της ίδιας απαίτησης εντός περιόδου 12 μηνών.

1.5 Για τους σκοπούς της παρούσας πολιτικής, ουσιώδης αλλαγή σημαίνει κάθε αλλαγή που επηρεάζει το πεδίο εφαρμογής του PIMS, τους σκοπούς επεξεργασίας PII, τις κατηγορίες PII, τις κατηγορίες υποκειμένων των δεδομένων προσωπικού χαρακτήρα, τις τοποθεσίες επεξεργασίας, την κατανομή ρόλων υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία, την αρχιτεκτονική συστημάτων, τις ρυθμίσεις με προμηθευτές ή υπεργολάβους επεξεργασίας, το προφίλ κινδύνου ιδιωτικότητας, τις εφαρμοστέες νομικές ή συμβατικές υποχρεώσεις, το πεδίο ελέγχου, τη μέθοδο παρακολούθησης ή το πεδίο πιστοποίησης.

2. Σκοπός

2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίσει ότι ο οργανισμός αξιολογεί την απόδοση του PIMS, επαληθεύει τη συμμόρφωση του PIMS, εντοπίζει μη συμμορφώσεις, διορθώνει αδυναμίες ελέγχων και βελτιώνει συνεχώς το PIMS με χρήση αντικειμενικών τεκμηρίων.

2.2 Η παρούσα πολιτική επιτρέπει στον οργανισμό να αποδεικνύει ότι οι δραστηριότητες παρακολούθησης, ελέγχου, ανασκόπησης της Διοίκησης και βελτίωσης του PIMS είναι σχεδιασμένες, ανεξάρτητες όπου απαιτείται, βασισμένες σε τεκμήρια, έγκαιρες και ιχνηλάσιμες προς υπόλογους ρόλους και κανονικά αντικείμενα τεκμηρίων.

3. Στόχοι

3.1 Οι στόχοι της παρούσας πολιτικής είναι οι εξής:

3.1.1 να καθορίσει ενοποιημένη διαδικασία παρακολούθησης και μέτρησης του PIMS·

3.1.2 να διασφαλίσει ότι οι στόχοι ιδιωτικότητας και η απόδοση των ελέγχων PIMS μετρώνται με χρήση τεκμηριωμένων τεκμηρίων·

3.1.3 να καθιερώσει πρόγραμμα εσωτερικών ελέγχων βάσει κινδύνου για το PIMS·

3.1.4 να διατηρήσει την ανεξαρτησία και την αντικειμενικότητα στις δραστηριότητες ελέγχου PIMS·

3.1.5 να διασφαλίσει ότι η ανασκόπηση της Διοίκησης λαμβάνει πλήρη και τρέχοντα δεδομένα εισόδου για την απόδοση του PIMS·

3.1.6 να διασφαλίσει ότι οι μη συμμορφώσεις καταγράφονται, αξιολογούνται, διορθώνονται και επαληθεύονται·

3.1.7 να διασφαλίσει ότι οι διορθωτικές ενέργειες παρακολουθούνται έως το κλείσιμο και ανασκοπούνται ως προς την αποτελεσματικότητά τους·

3.1.8 να εντοπίσει επαναλαμβανόμενες αδυναμίες και ευκαιρίες βελτίωσης·

3.1.9 να υποστηρίξει την ετοιμότητα για πιστοποίηση και την υπόλογη διαχείριση τεκμηρίων·

3.1.10 να αποφύγει την επικάλυψη επιχειρησιακών μετρικών που έχουν ήδη καθοριστεί σε συναφείς πολιτικές PIMS.

4. Δηλώσεις πολιτικής

4.1 Πλαίσιο παρακολούθησης και μέτρησης PIMS

4.1.1 [Both] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ καθορίζει το ενοποιημένο πρόγραμμα παρακολούθησης PIMS στο REG12 πριν από την αρχική λειτουργία του PIMS και ετησίως στη συνέχεια.

4.1.2 [Both] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ καθορίζει τη μέθοδο μέτρησης, τη συχνότητα, την πηγή τεκμηρίων, τον στόχο και τον υπεύθυνο ρόλο για κάθε μετρική PIMS στο REG12 πριν από την έναρξη του κύκλου μέτρησης.

4.1.3 [Both] Ο ρόλος Process Owner / Business Owner ΠΡΕΠΕΙ ΝΑ παρέχει δεδομένα εισόδου παρακολούθησης δραστηριοτήτων επεξεργασίας PII από το REG02 στον ρόλο Privacy Lead / PIMS Manager ανά τρίμηνο.

4.1.4 [Both] Ο ρόλος Information Security Lead ΠΡΕΠΕΙ ΝΑ παρέχει δεδομένα εισόδου κατάστασης ελέγχων ασφάλειας PII από το REG03 στον ρόλο Privacy Lead / PIMS Manager ανά τρίμηνο.

4.1.5 [Both] Ο ρόλος Vendor / Procurement Owner ΠΡΕΠΕΙ ΝΑ παρέχει δεδομένα εισόδου για την κατάσταση εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας, κοινοχρησίας με τρίτα μέρη και διασφάλισης προμηθευτών από το REG08 στον ρόλο Privacy Lead / PIMS Manager ανά τρίμηνο.

4.1.6 [All] Ο ρόλος Incident Response Coordinator ΠΡΕΠΕΙ ΝΑ παρέχει δεδομένα εισόδου για τάσεις περιστατικών ιδιωτικότητας και παραβιάσεων από το REG10 στον ρόλο Privacy Lead / PIMS Manager μηνιαίως και εντός 10 εργάσιμων ημερών μετά το κλείσιμο μείζονος περιστατικού.

4.1.7 [Both] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ ενοποιεί τα αποτελέσματα παρακολούθησης PIMS στο REG12 ανά τρίμηνο.

4.2 Πρόγραμμα εσωτερικών ελέγχων PIMS

4.2.1 [All] Ο ρόλος Internal Audit / Compliance Reviewer ΠΡΕΠΕΙ ΝΑ καταρτίζει πρόγραμμα εσωτερικών ελέγχων PIMS βάσει κινδύνου στο REG12 ετησίως πριν από τον πρώτο προγραμματισμένο κύκλο ελέγχου PIMS.

4.2.2 [All] Ο ρόλος Internal Audit / Compliance Reviewer ΠΡΕΠΕΙ ΝΑ καθορίζει τον στόχο, τα κριτήρια, το πεδίο εφαρμογής, τη μέθοδο, τη βάση δειγματοληψίας και την προθεσμία αναφοράς για κάθε έλεγχο PIMS στο REG12 πριν από την έναρξη των επιτόπιων ελεγκτικών εργασιών.

4.2.3 [All] Ο ρόλος Internal Audit / Compliance Reviewer ΠΡΕΠΕΙ ΝΑ καταγράφει τους ελέγχους ανεξαρτησίας ελεγκτή και σύγκρουσης συμφερόντων στο REG12 πριν από κάθε ανάθεση ελέγχου.

4.2.4 [All] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ καθιστά διαθέσιμες τις ζητούμενες ελεγχόμενες τεκμηριωμένες πληροφορίες PIMS και τα τεκμήρια μητρώων μέσω του REG12 εντός 10 εργάσιμων ημερών από εγκεκριμένο αίτημα ελέγχου.

4.2.5 [Both] Ο ρόλος Internal Audit / Compliance Reviewer ΠΡΕΠΕΙ ΝΑ ελέγχει την εφαρμοστέα κατάσταση υλοποίησης ελέγχων PIMS έναντι του REG03 κατά τη διάρκεια κάθε ελέγχου PIMS.

4.2.6 [Both] Ο ρόλος Internal Audit / Compliance Reviewer ΠΡΕΠΕΙ ΝΑ καταγράφει το επιλεγμένο δείγμα τεκμηρίων επεξεργασίας PII στο REG12 κατά τη διάρκεια κάθε ελέγχου PIMS.

4.2.7 [All] Ο ρόλος Internal Audit / Compliance Reviewer ΠΡΕΠΕΙ ΝΑ καταγράφει τα αποτελέσματα ελέγχου PIMS στο REG12 εντός 15 εργάσιμων ημερών μετά την ολοκλήρωση του ελέγχου.

4.2.8 [All] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ αναθέτει υπευθύνους διορθωτικών ενεργειών για αποδεκτά ευρήματα ελέγχου PIMS στο REG12 εντός 10 εργάσιμων ημερών από την αποδοχή των αποτελεσμάτων ελέγχου.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Εξαιρέσεις

9.1 Εξαιρέσεις παρακολούθησης, ελέγχου και βελτίωσης

9.1.1 [All] Ο ρόλος Process Owner / Business Owner ΠΡΕΠΕΙ ΝΑ ζητά κάθε εξαίρεση από την παρούσα πολιτική στο REG12 πριν από την απόκλιση.

9.1.2 [All] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ αξιολογεί τον αντίκτυπο κάθε ζητούμενης εξαίρεσης στην ιδιωτικότητα, την πιστοποίηση, τον έλεγχο και τις διορθωτικές ενέργειες στο REG12 εντός 10 εργάσιμων ημερών από το αίτημα.

9.1.3 [All] Ο ρόλος Data Protection Officer / Privacy Advisor ΠΡΕΠΕΙ ΝΑ καταγράφει συμβουλές στο REG12 πριν από την έγκριση κάθε εξαίρεσης που επηρεάζει νομικές υποχρεώσεις, δικαιώματα υποκειμένων των δεδομένων προσωπικού χαρακτήρα, δεσμεύσεις DPIA, υποχρεώσεις ελέγχου πελάτη ή επεξεργασία υψηλού κινδύνου.

9.1.4 [All] Το Top Management ΠΡΕΠΕΙ ΝΑ εγκρίνει εξαιρέσεις που επηρεάζουν την ολοκλήρωση χρονοδιαγράμματος ελέγχων, την ανασκόπηση της Διοίκησης, μείζονες μη συμμορφώσεις, το πεδίο πιστοποίησης ή την επεξεργασία υψηλού κινδύνου στο REG12 πριν από την έναρξη ισχύος της εξαίρεσης.

9.1.5 [All] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ ορίζει ημερομηνία λήξης που δεν υπερβαίνει τις 90 ημέρες στο REG12 για κάθε εγκεκριμένη εξαίρεση παρακολούθησης, ελέγχου ή βελτίωσης.

9.1.6 [All] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ κλείνει ή να επαναξιολογεί κάθε εξαίρεση παρακολούθησης, ελέγχου ή βελτίωσης στο REG12 εντός πέντε εργάσιμων ημερών από τη λήξη.

10. Εφαρμογή

10.1 Εφαρμογή των απαιτήσεων παρακολούθησης, ελέγχου και βελτίωσης

10.1.1 [All] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ καταγράφει ως μη συμμόρφωση στο REG12 έναν χαμένο κύκλο παρακολούθησης, έναν μη διενεργηθέντα έλεγχο PIMS, εκπρόθεσμη ανασκόπηση της Διοίκησης, ελλείποντα ελεγκτικά τεκμήρια, εκπρόθεσμη

διορθωτική ενέργεια ή εκπρόθεσμη ενέργεια βελτίωσης εντός πέντε εργάσιμων ημερών από τον εντοπισμό.

10.1.2 [All] Ο ρόλος Internal Audit / Compliance Reviewer ΠΡΕΠΕΙ ΝΑ καταγράφει τη σοβαρότητα ευρημάτων ελέγχου στο REG12 πριν από την έκδοση της αναφοράς ελέγχου.

10.1.3 [All] Το Top Management ΠΡΕΠΕΙ ΝΑ απαιτεί διορθωτική ενέργεια για κάθε μείζονα μη συμμόρφωση PIMS στο REG12 εντός 10 εργάσιμων ημερών από την κλιμάκωση.

10.1.4 [All] Ο ρόλος Process Owner / Business Owner ΠΡΕΠΕΙ ΝΑ αποτρέπει τη θέση σε λειτουργία ή την υποβολή εξωτερικής διασφάλισης για επεξεργασία υψηλού κινδύνου όταν τα απαιτούμενα τεκμήρια διορθωτικής ενέργειας απουσιάζουν από το REG12 πριν από τη θέση σε λειτουργία ή την υποβολή.

10.1.5 [All] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ κλιμακώνει επαναλαμβανόμενες χαμένες προθεσμίες παρακολούθησης ή διορθωτικών ενεργειών στο Top Management στο REG12 εντός πέντε εργάσιμων ημερών μετά τη δεύτερη εμφάνιση εντός περιόδου 12 μηνών.

10.1.6 [All] Ο ρόλος Internal Audit / Compliance Reviewer ΠΡΕΠΕΙ ΝΑ επαληθεύει το κλείσιμο ενεργειών εφαρμογής στο REG12 στον επόμενο προγραμματισμένο έλεγχο ή εντός 60 ημερών από το αναφερόμενο κλείσιμο, όποιο επέλθει πρώτο.

11. Ανασκόπηση και συντήρηση

11.1 Ανασκόπηση και συντήρηση πολιτικής

11.1.1 [All] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ ανασκοπεί την παρούσα πολιτική στο REG12 ετησίως και εντός 30 ημερών από ουσιώδη αλλαγή στις απαιτήσεις παρακολούθησης, ελέγχου, ανασκόπησης της Διοίκησης, διορθωτικών ενεργειών ή πιστοποίησης του PIMS.

11.1.2 [All] Ο ρόλος Internal Audit / Compliance Reviewer ΠΡΕΠΕΙ ΝΑ ανασκοπεί την αποτελεσματικότητα του προγράμματος ελέγχων PIMS στο REG12 ετησίως μετά τον τελικό προγραμματισμένο έλεγχο για το έτος λειτουργίας του PIMS.

11.1.3 [All] Ο ρόλος Data Protection Officer / Privacy Advisor ΠΡΕΠΕΙ ΝΑ ανασκοπεί αλλαγές σημαντικές για την ιδιωτικότητα στην παρούσα πολιτική στο REG12 πριν από την έγκριση.

11.1.4 [All] Το Top Management ΠΡΕΠΕΙ ΝΑ εγκρίνει ουσιώδεις αλλαγές στην παρούσα πολιτική στο REG12 πριν από τη δημοσίευση.

11.1.5 [All] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ επικαιροποιεί τα REG01 και REG03 εντός 15 εργάσιμων ημερών μετά από εγκεκριμένες αλλαγές στην παρούσα πολιτική που μεταβάλλουν το πεδίο εφαρμογής του PIMS ή την εφαρμοσιμότητα ελέγχων.

11.1.6 [All] Ο ρόλος Privacy Lead / PIMS Manager ΠΡΕΠΕΙ ΝΑ καταγράφει την επικοινωνία εγκεκριμένων αλλαγών στην παρούσα πολιτική στο REG11 εντός 30 ημερών από τη δημοσίευση.

12. Συναφείς πολιτικές

12.1 Η παρούσα πολιτική υποστηρίζεται από τις ακόλουθες συναφείς πολιτικές:

12.2 PII01 - Πολιτική Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας

12.3 PII02 - Πολιτική Ρόλων, Αρμοδιοτήτων και Λογοδοσίας Ιδιωτικότητας

12.4 PII03 - Πολιτική Απογραφής Επεξεργασίας PII και Νομικής Βάσης

12.5 PII04 - Πολιτική Ειδοποίησης Ιδιωτικότητας και Διαφάνειας

12.6 PII05 - Πολιτική Διαχείρισης Συγκατάθεσης και Προτιμήσεων

12.7 PII06 - Πολιτική Διαχείρισης Δικαιωμάτων Υποκειμένων των Δεδομένων Προσωπικού Χαρακτήρα

12.8 PII07 - Πολιτική Αξιολόγησης Κινδύνου Ιδιωτικότητας και DPIA

12.9 PII08 - Πολιτική Προστασίας της Ιδιωτικότητας ήδη από τον Σχεδιασμό και εξ Ορισμού

12.10 PII09 - Πολιτική Συλλογής, Χρήσης, Κοινολόγησης και Κοινοχρησίας PII

12.11 PII10 - Πολιτική Διατήρησης, Διαγραφής και Διάθεσης PII

12.12 PII11 - Πολιτική Ακρίβειας και Ποιότητας PII

12.13 PII12 - Πολιτική Διαχείρισης Ιδιωτικότητας Εκτελούντων την Επεξεργασία, Υπεργολάβων Επεξεργασίας και Τρίτων Μερών

12.14 PII13 - Πολιτική Διεθνούς Διαβίβασης PII

12.15 PII14 - Πολιτική Ασφάλειας PII και Ελέγχου Πρόσβασης

12.16 PII15 - Πολιτική Διαχείρισης Περιστατικών και Παραβιάσεων PII

12.17 PII16 - Πολιτική Εκπαίδευσης, Ευαισθητοποίησης και Επάρκειας σε Θέματα Ιδιωτικότητας

12.18 PII17 - Πολιτική Τεκμηριωμένων Πληροφοριών και Διαχείρισης Τεκμηρίων PIMS

13. Πρότυπα και πλαίσια αναφοράς

13.1 Η παρούσα πολιτική αντιστοιχίζεται στα ακόλουθα πρότυπα και κανονισμούς. Η αντιστοίχιση εξηγεί πώς η πολιτική υποστηρίζει τις αναφερόμενες απαιτήσεις και προσδιορίζει τις εσωτερικές ρήτρες που τις υλοποιούν ή τις υποστηρίζουν.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Αντιστοιχίζεται στον καθορισμό, τη μέτρηση, την αναφορά και την ανασκόπηση των στόχων PIMS και των μετρικών απόδοσης PIMS. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Αντιστοιχίζεται στην τήρηση τεκμηριωμένων πληροφοριών για αποτελέσματα παρακολούθησης, προγράμματα ελέγχων, αποτελέσματα ελέγχων, τεκμήρια ανασκόπησης της Διοίκησης, μη συμμορφώσεις, διορθωτικές ενέργειες και ενέργειες βελτίωσης. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Αντιστοιχίζεται στη λειτουργία του σχεδιασμένου κύκλου παρακολούθησης, ελέγχου, διορθωτικών ενεργειών και βελτίωσης PIMS ως μέρος του επιχειρησιακού ελέγχου του PIMS. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Αντιστοιχίζεται στον καθορισμό του τι παρακολουθείται και μετράται, στην ενοποίηση αποτελεσμάτων παρακολούθησης, στην αξιολόγηση της απόδοσης του PIMS και στην τήρηση τεκμηρίων μέτρησης. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Αντιστοιχίζεται στην τήρηση του προγράμματος εσωτερικών ελέγχων, στον σχεδιασμό ελέγχων, στους ελέγχους ανεξαρτησίας ελεγκτή, στη δειγματοληψία τεκμηρίων, στα αποτελέσματα ελέγχων και στην παρακολούθηση ευρημάτων ελέγχου. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Αντιστοιχίζεται στον σχεδιασμό ανασκόπησης της Διοίκησης, στην ανασκόπηση της απόδοσης του PIMS, στην ανασκόπηση τάσεων ελέγχων και διορθωτικών ενεργειών, στην έγκριση αποτελεσμάτων και στις αποφάσεις πόρων. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Αντιστοιχίζεται στον εντοπισμό, την έγκριση, την υλοποίηση και την παρακολούθηση ευκαιριών συνεχούς βελτίωσης για την καταλληλότητα, την επάρκεια και την αποτελεσματικότητα του PIMS. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Αντιστοιχίζεται στην καταγραφή μη συμμορφώσεων, στην ανάλυση βασικής αιτίας, στον σχεδιασμό διορθωτικών ενεργειών, στην υλοποίηση διορθωτικών ενεργειών, στην επαλήθευση αποτελεσματικότητας, στην κλιμάκωση και στην εφαρμογή. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Αντιστοιχίζεται στα αρχεία επεξεργασίας υπευθύνου επεξεργασίας που χρησιμοποιούνται ως πηγές τεκμηρίων για παρακολούθηση, δειγματοληψία ελέγχου και μετρικές επικαιρότητας απογραφής επεξεργασίας. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Αντιστοιχίζεται σε συμφωνίες εκτελούντων την επεξεργασία, ελέγχους πελατών, αποκρίσεις διασφάλισης και τεκμήρια συνεργασίας εκτελούντων την επεξεργασία που παρακολουθούνται μέσω διαδικασιών διασφάλισης προμηθευτών και πελατών. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Αντιστοιχίζεται σε τεκμήρια λογοδοσίας για παρακολούθηση, έλεγχο, ανασκόπηση της Διοίκησης, διορθωτικές ενέργειες και συνεχή βελτίωση. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Αντιστοιχίζεται σε μέτρα διακυβέρνησης υπευθύνου επεξεργασίας, ανασκόπηση αποτελεσματικότητας, ανασκόπηση της Διοίκησης, διορθωτικές ενέργειες και τεκμηριωμένα τεκμήρια βελτίωσης. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Αντιστοιχίζεται σε τεκμήρια εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας, ελέγχων πελατών, διασφάλισης τρίτων μερών και συνεργασίας προμηθευτών. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Αντιστοιχίζεται σε αρχεία επεξεργασίας που χρησιμοποιούνται ως τεκμήρια παρακολούθησης, δειγματοληψίας ελέγχου, πληρότητας αντικειμένων τεκμηρίων και επικαιρότητας απογραφής επεξεργασίας. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Αντιστοιχίζεται στην παρακολούθηση και αξιολόγηση της κατάστασης ελέγχων ασφάλειας PII, των τεκμηρίων τεχνικών ελέγχων και των τεκμηρίων αποτελεσματικότητας που σχετίζονται με την ασφάλεια. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Αντιστοιχίζεται σε συμβουλές ιδιωτικότητας, παρατηρήσεις παρακολούθησης, υποστήριξη ελέγχων και ανασκόπηση τάσεων συμμόρφωσης ιδιωτικότητας από τον Data Protection Officer / Privacy Advisor, όπου εφαρμόζεται. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Αντιστοιχίζεται στην επαλήθευση συμμόρφωσης ιδιωτικότητας, στους εσωτερικούς ή ανεξάρτητους ελέγχους, στους εσωτερικούς ελέγχους, στους μηχανισμούς εποπτείας και στα τεκμήρια αξιολόγησης κινδύνου ιδιωτικότητας. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Αντιστοιχίζεται στην ανεξάρτητη ανασκόπηση της ασφάλειας πληροφοριών που σχετίζεται με PII, στη συμμόρφωση με πολιτικές και πρότυπα και στην τεχνική ανασκόπηση συμμόρφωσης για την προστασία PII. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Αντιστοιχίζεται σε δεδομένα εισόδου παρακολούθησης και αξιολόγησης ασφάλειας πληροφοριών που υποστηρίζουν τη μέτρηση απόδοσης του PIMS και την κατάσταση ελέγχων ασφάλειας PII. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Αντιστοιχίζεται στην υποστήριξη εσωτερικού ελέγχου ISMS για τον σχεδιασμό ελέγχων PIMS, τα τεκμήρια ελέγχου, τα αποτελέσματα ελέγχων και την ολοκλήρωση του προγράμματος ελέγχων. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Αντιστοιχίζεται σε δεδομένα εισόδου και αποτελέσματα ανασκόπησης της Διοίκησης για ενιαία εποπτεία της απόδοσης PIMS και ασφάλειας πληροφοριών. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Αντιστοιχίζεται στη συνεχή βελτίωση του PIMS και του υποστηρικτικού περιβάλλοντος ελέγχων ασφάλειας πληροφοριών. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Αντιστοιχίζεται στη διαχείριση μη συμμόρφωσης, στον σχεδιασμό διορθωτικών ενεργειών, στην υλοποίηση διορθωτικών ενεργειών και στην επαλήθευση αποτελεσματικότητας. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Αντιστοιχίζεται στην ανεξάρτητη ανασκόπηση, στους ελέγχους ανεξαρτησίας ελεγκτή, στη δοκιμή ελεγκτικών τεκμηρίων και στην ανεξάρτητη επαλήθευση της αποτελεσματικότητας διορθωτικών ενεργειών. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Αντιστοιχίζεται στην ανασκόπηση συμμόρφωσης πολιτικών PIMS και ασφάλειας πληροφοριών, στην κατάσταση υλοποίησης ελέγχων και στα τεκμήρια συμμόρφωσης με πρότυπα. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Αντιστοιχίζεται στις αρχές ελέγχου, στη διαχείριση προγράμματος ελέγχων, στη διεξαγωγή ελέγχων, στην αναφορά ελέγχων βάσει τεκμηρίων, στην παρακολούθηση ελέγχων και στις προσδοκίες επάρκειας ελεγκτών για ελέγχους PIMS. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].