					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: PII16					Τίτλος εγγράφου: **Πολιτική εκπαίδευσης, ευαισθητοποίησης και επάρκειας σε θέματα ιδιωτικότητας**							
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 / Έλεγχος / Άρθρο	Εφαρμοσιμότητα	Τύπος κάλυψης	Σχόλιο
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Επάρκεια και ευαισθητοποίηση
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Επικοινωνία και τεκμηριωμένα τεκμήρια
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Επιχειρησιακός έλεγχος, μέτρηση και βελτίωση
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Ευαισθητοποίηση, εκπαίδευση και κατάρτιση σχετικά με την επεξεργασία PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Λογοδοσία, διακυβέρνηση εκτελούντων την επεξεργασία, ασφάλεια και καθήκοντα DPO
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Επάρκεια, ευαισθητοποίηση και εκπαίδευση
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Καθοδήγηση για ευαισθητοποίηση, εκπαίδευση και κατάρτιση
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Ασφάλεια πληροφοριών και συμμόρφωση σε θέματα ιδιωτικότητας

1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική καθορίζει τις απαιτήσεις του οργανισμού για την εκπαίδευση, την ευαισθητοποίηση και την επάρκεια σε θέματα ιδιωτικότητας εντός του Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας.

1.2 Η παρούσα πολιτική εφαρμόζεται στο προσωπικό, στους αναδόχους, στο προσωρινό προσωπικό, στα σχετικά τρίτα μέρη, στους εκτελούντες την επεξεργασία, στους υπεργολάβους επεξεργασίας και σε άλλα ενδιαφερόμενα μέρη των οποίων η εργασία μπορεί να επηρεάσει την επεξεργασία PII, την απόδοση του PIMS, τα δικαιώματα των υποκειμένων των δεδομένων προσωπικού χαρακτήρα, τον κίνδυνο ιδιωτικότητας, την ασφάλεια πληροφοριών που σχετίζεται με PII, τις εντολές εκτελούντος την επεξεργασία, τα περιστατικά ιδιωτικότητας, τις τεκμηριωμένες πληροφορίες ή τα τεκμήρια συμμόρφωσης.

1.3 Η παρούσα πολιτική εφαρμόζεται σε πλαίσια υπευθύνου επεξεργασίας, από κοινού υπευθύνου επεξεργασίας, εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας.

1.4 Η παρούσα πολιτική καλύπτει:

1.4.1 τον προσδιορισμό των αποδεκτών της εκπαίδευσης σε θέματα ιδιωτικότητας·

1.4.2 την εκπαίδευση κατά την ένταξη·

1.4.3 την ετήσια επαναληπτική εκπαίδευση·

1.4.4 την εκπαίδευση βάσει ρόλων και την εκπαίδευση που ενεργοποιείται από γεγονότα·

1.4.5 τα τεκμήρια ολοκλήρωσης εκπαίδευσης·

1.4.6 την κλιμάκωση μη ολοκλήρωσης·

1.4.7 την ανασκόπηση της αποτελεσματικότητας της εκπαίδευσης·

1.4.8 τα τεκμήρια διασφάλισης εκπαίδευσης εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών.

1.5 Η παρούσα πολιτική δεν δημιουργεί χωριστή μήτρα εκπαίδευσης, πίνακα ελέγχου εκπαίδευσης, μητρώο ανθρώπινου δυναμικού, μητρώο επάρκειας, πειθαρχικό μητρώο ή μητρώο εκπαίδευσης πελατών. Οι αναθέσεις εκπαίδευσης, οι ολοκληρώσεις, οι υπενθυμίσεις, τα τεκμήρια επάρκειας και τα τεκμήρια ευαισθητοποίησης καταγράφονται στο REG11, ενώ οι εξαιρέσεις, οι κλιμακώσεις, οι μη συμμορφώσεις, οι διορθωτικές ενέργειες και τα τεκμήρια ανασκόπησης καταγράφονται στο REG12. Τα τεκμήρια διασφάλισης εκπαίδευσης εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών καταγράφονται στο REG08, όπου είναι σχετικό.

1.6 Η παρούσα πολιτική δεν επαναλαμβάνει:

1.6.1 την ανάθεση λογοδοσίας ανά ρόλο στο PII02·

1.6.2 τις απαιτήσεις απογραφής επεξεργασιών και νομικής βάσης στο PII03·

1.6.3 τη μεθοδολογία κινδύνου ιδιωτικότητας και DPIA στο PII07·

1.6.4 τις πύλες προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό στο PII08·

1.6.5 τη διακυβέρνηση του κύκλου ζωής εκτελούντων την επεξεργασία στο PII12·

1.6.6 τη λειτουργία ασφάλειας και ελέγχου πρόσβασης για PII στο PII14·

1.6.7 τη ροή εργασίας περιστατικών και παραβιάσεων PII στο PII15·

1.6.8 τη διακυβέρνηση τεκμηριωμένων πληροφοριών στο PII17·

1.6.9 τη διακυβέρνηση παρακολούθησης, εσωτερικού ελέγχου και βελτίωσης στο PII18.

2. Σκοπός

2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίζει ότι τα άτομα των οποίων η εργασία επηρεάζει την επεξεργασία PII κατανοούν τις αρμοδιότητές τους σε θέματα ιδιωτικότητας, ολοκληρώνουν κατάλληλη εκπαίδευση με καθορισμένη συχνότητα, διατηρούν επάρκεια σχετική με τον ρόλο τους και παράγουν ελέγξιμα τεκμήρια εκπαίδευσης, ευαισθητοποίησης και κλιμάκωσης.

2.2 Η παρούσα πολιτική υποστηρίζει τη συνεπή εφαρμογή του PIMS, χρησιμοποιώντας το REG11 ως το κύριο αντικείμενο τεκμηρίωσης εκπαίδευσης και ευαισθητοποίησης και τα REG08, REG10 και REG12 ως υποστηρικτικά αντικείμενα τεκμηρίωσης.

3. Στόχοι

3.1 Οι στόχοι της παρούσας πολιτικής είναι να:

3.1.1 καθορίζει τους αποδέκτες της εκπαίδευσης σε θέματα ιδιωτικότητας·

3.1.2 καθορίζει τις απαιτήσεις εκπαίδευσης κατά την ένταξη·

3.1.3 καθορίζει τις απαιτήσεις ετήσιας επαναληπτικής εκπαίδευσης·

3.1.4 καθορίζει τις απαιτήσεις εκπαίδευσης σε θέματα ιδιωτικότητας βάσει ρόλων·

3.1.5 καταγράφει τα τεκμήρια ολοκλήρωσης στο REG11·

3.1.6 κλιμακώνει τη μη ολοκλήρωση μέσω του REG12·

3.1.7 διατηρεί τεκμήρια διασφάλισης εκπαίδευσης εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών στο REG08, όπου είναι σχετικό·

3.1.8 ανασκοπεί την αποτελεσματικότητα της εκπαίδευσης χωρίς να δημιουργεί υπερβολικές μετρικές ή διπλά μητρώα·

3.1.9 διασφαλίζει ότι το περιεχόμενο εκπαίδευσης παραμένει ευθυγραμμισμένο με τις ισχύουσες πολιτικές PIMS και με ουσιώδεις υποχρεώσεις ιδιωτικότητας.

4. Δηλώσεις πολιτικής

4.1 Αποδέκτες της εκπαίδευσης και ανάθεση εκπαίδευσης

4.1.1 [All] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να καθορίζει τις κατηγορίες αποδεκτών της εκπαίδευσης PIMS στο REG11 πριν από την έναρξη κάθε ετήσιου κύκλου εκπαίδευσης.

4.1.2 [All] Ο Process Owner / Business Owner ΠΡΕΠΕΙ να προσδιορίζει στο REG11 το προσωπικό του οποίου τα καθήκοντα περιλαμβάνουν επεξεργασία PII πριν από την ένταξη, την ανάθεση ρόλου ή την ουσιώδη αλλαγή καθηκόντων.

4.1.3 [Conditional] Ο System Owner / Application Owner ΠΡΕΠΕΙ να προσδιορίζει στο REG11 τους χρήστες που απαιτούν εκπαίδευση ιδιωτικότητας για σύστημα PII, προνομιούχα πρόσβαση ή διοικητική πρόσβαση πριν ενεργοποιηθεί ή μεταβληθεί ουσιωδώς η πρόσβαση.

4.1.4 [Joint Controller] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να καταγράφει την κατανομή ευθυνών εκπαίδευσης από κοινού υπευθύνων επεξεργασίας στο REG11 ή στο REG08 πριν από την έναρξη ή την ουσιώδη αλλαγή της κοινής δραστηριότητας επεξεργασίας.

4.1.5 [Conditional] Ο Data Protection Officer / Privacy Advisor ΠΡΕΠΕΙ να προσδιορίζει τις ανάγκες ενισχυμένης εκπαίδευσης σε θέματα ιδιωτικότητας στο REG11 πριν ανατεθεί εκπαίδευση σε ρόλους που χειρίζονται επεξεργασία υψηλού κινδύνου, PII ειδικών κατηγοριών, δικαιώματα υποκειμένων των δεδομένων προσωπικού χαρακτήρα, DPIAs, διεθνείς διαβιβάσεις ή αξιολόγηση παραβίασης.

4.1.6 [All] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να καταγράφει στο REG11 τους ανατεθειμένους αποδέκτες της εκπαίδευσης, τον τύπο εκπαίδευσης, την απαιτούμενη ημερομηνία ολοκλήρωσης και τον υπεύθυνο τεκμηρίων πριν από την έναρξη κάθε ετήσιου κύκλου εκπαίδευσης.

4.2 Συχνότητα εκπαίδευσης κατά την ένταξη και ετήσιας εκπαίδευσης

4.2.1 [All] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να αναθέτει βασική εκπαίδευση ευαισθητοποίησης σε θέματα ιδιωτικότητας στο REG11 εντός 10 εργάσιμων ημερών από την ένταξη για προσωπικό με πρόσβαση σε PII ή με αρμοδιότητες PIMS.

4.2.2 [All] Ο Process Owner / Business Owner ΠΡΕΠΕΙ να διασφαλίζει ότι το ανατεθειμένο προσωπικό ολοκληρώνει την εκπαίδευση ιδιωτικότητας κατά την ένταξη στο REG11 πριν

εγκριθεί μη εποπτευόμενη πρόσβαση σε PII ή εντός 30 ημερών από την ένταξη, όποιο συμβεί πρώτο.

4.2.3 [All] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να αναθέτει ετήσια επαναληπτική εκπαίδευση σε θέματα ιδιωτικότητας στο REG11 τουλάχιστον μία φορά κάθε 12 μήνες.

4.2.4 [All] Ο Process Owner / Business Owner ΠΡΕΠΕΙ να επιβεβαιώνει την κατάσταση ολοκλήρωσης της ετήσιας επαναληπτικής εκπαίδευσης για το ανατεθειμένο προσωπικό στο REG11 έως τη δημοσιευμένη ετήσια καταληκτική ημερομηνία.

4.2.5 [Conditional] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να αναθέτει στοχευμένη επαναληπτική εκπαίδευση στο REG11 εντός 30 ημερών μετά από ουσιώδη αλλαγή πολιτικής ιδιωτικότητας, ουσιώδη αλλαγή διεργασίας PIMS, εύρημα ελέγχου, επαναλαμβανόμενη αποτυχία εκπαίδευσης ή σχετικό δίδαγμα από περιστατικό PII.

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

9. Εξαιρέσεις

9.1.1 [All] Ο Process Owner / Business Owner ΠΡΕΠΕΙ να καταγράφει αίτημα εξαίρεσης εκπαίδευσης σε θέματα ιδιωτικότητας στο REG12 πριν παραταθεί απαιτούμενη προθεσμία ολοκλήρωσης.

9.1.2 [All] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να εγκρίνει ή να απορρίπτει αιτήματα εξαίρεσης εκπαίδευσης σε θέματα ιδιωτικότητας στο REG12 πριν η εξαίρεση καταστεί ενεργή.

9.1.3 [Conditional] Ο Data Protection Officer / Privacy Advisor ΠΡΕΠΕΙ να παρέχει συμβουλές για εξαιρέσεις εκπαίδευσης στο REG12 πριν από την έγκριση, όταν η εξαίρεση επηρεάζει επεξεργασία υψηλού κινδύνου, PII ειδικών κατηγοριών, χειρισμό δικαιωμάτων, χειρισμό περιστατικών, διεθνείς διαβιβάσεις ή τεκμήρια πιστοποίησης.

9.1.4 [Conditional] Η Top Management ΠΡΕΠΕΙ να εγκρίνει εξαιρέσεις εκπαίδευσης σε θέματα ιδιωτικότητας στο REG12 πριν από την ενεργοποίηση, όταν η εξαίρεση επηρεάζει επαναλαμβανόμενη μη ολοκλήρωση, προνομιούχα πρόσβαση σε PII, επεξεργασία PII υψηλού αντικτύπου ή τεκμήρια προς ρυθμιστικές αρχές.

9.1.5 [All] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να καθορίζει στο REG12 τον ιδιοκτήτη εξαίρεσης, την ημερομηνία λήξης, την αντισταθμιστική ενέργεια και την ημερομηνία ανασκόπησης πριν εγκρίνει οποιαδήποτε εξαίρεση εκπαίδευσης σε θέματα ιδιωτικότητας.

9.1.6 [All] Ο Process Owner / Business Owner ΠΡΕΠΕΙ να κλείνει ή να ανανεώνει εγκεκριμένες εξαιρέσεις εκπαίδευσης σε θέματα ιδιωτικότητας στο REG12 πριν από την ημερομηνία λήξης της εξαίρεσης.

10. Εφαρμογή και τήρηση

10.1.1 [All] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να καταγράφει μη συμμόρφωση εκπαίδευσης στο REG12 εντός πέντε εργάσιμων ημερών όταν τα τεκμήρια υποχρεωτικής εκπαίδευσης σε θέματα ιδιωτικότητας λείπουν, είναι ελλιπή, εκπρόθεσμα ή δεν είναι ιχνηλάσιμα στο REG11.

10.1.2 [All] Ο Process Owner / Business Owner ΠΡΕΠΕΙ να διασφαλίζει ότι η εκπρόθεσμη υποχρεωτική εκπαίδευση σε θέματα ιδιωτικότητας ολοκληρώνεται ή κλιμακώνεται στο REG11 ή στο REG12 εντός 10 εργάσιμων ημερών μετά την καταγραφή της εκπρόθεσμης κατάστασης.

10.1.3 [Conditional] Ο System Owner / Application Owner ΠΡΕΠΕΙ να περιορίζει νέα πρόσβαση υψηλού αντικτύπου σε PII στο REG12 όταν η απαιτούμενη εκπαίδευση ιδιωτικότητας κατά την ένταξη ή βάσει ρόλων παραμένει ελλιπής μετά την κλιμάκωση.

10.1.4 [Processor] Ο Vendor / Procurement Owner ΠΡΕΠΕΙ να κλιμακώνει ελλείποντα τεκμήρια διασφάλισης εκπαίδευσης εκτελούντος την επεξεργασία, υπεργολάβου επεξεργασίας ή

εξωτερικού εργατικού δυναμικού στο REG08 και στο REG12 εντός πέντε εργάσιμων ημερών από τον εντοπισμό τους.

10.1.5 [Conditional] Ο Incident Response Coordinator ΠΡΕΠΕΙ να συνδέει ενέργειες εφαρμογής που σχετίζονται με την εκπαίδευση με το REG10 εντός μίας εργάσιμης ημέρας όταν η αποτυχία εκπαίδευσης συνέβαλε σε ύποπτο ή επιβεβαιωμένο περιστατικό PII.

10.1.6 [All] Ο Internal Audit / Compliance Reviewer ΠΡΕΠΕΙ να επαληθεύει τεκμήρια κλεισίματος για διορθωτικές ενέργειες εκπαίδευσης στο REG12 στον επόμενο προγραμματισμένο έλεγχο ή εντός 60 ημερών από το κλείσιμο, όποιο συμβεί πρώτο.

11. Ανασκόπηση και συντήρηση

11.1.1 [All] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να ανασκοπεί την παρούσα πολιτική και το περιεχόμενο εκπαίδευσης τουλάχιστον ετησίως και να καταγράφει το αποτέλεσμα της ανασκόπησης στο REG11 ή στο REG12.

11.1.2 [All] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να ανασκοπεί την παρούσα πολιτική εντός 30 ημερών μετά από ουσιώδη αλλαγή στο πεδίο εφαρμογής του PIMS, στη νομοθεσία περί ιδιωτικότητας, στις δραστηριότητες επεξεργασίας, στο μοντέλο ρόλων, στα διδάγματα από περιστατικά, στα ευρήματα ελέγχου ή στα αποτελέσματα αποτελεσματικότητας της εκπαίδευσης.

11.1.3 [Conditional] Ο Data Protection Officer / Privacy Advisor ΠΡΕΠΕΙ να ανασκοπεί στο REG12 αλλαγές πολιτικής που είναι σημαντικές για την ιδιωτικότητα πριν από την έγκριση.

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

11.1.5 [All] Ο Privacy Lead / PIMS Manager ΠΡΕΠΕΙ να επικαιροποιεί το περιεχόμενο εκπαίδευσης και τα τεκμήρια ανάθεσης στο REG11 εντός 30 ημερών μετά από εγκεκριμένη ουσιώδη αλλαγή πολιτικής.

12. Συναφείς πολιτικές

12.1 Η παρούσα πολιτική θα πρέπει να διαβάζεται σε συνδυασμό με:

12.2 PII01 - Πολιτική Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας·

12.3 PII02 - Πολιτική ρόλων, αρμοδιοτήτων και λογοδοσίας για την ιδιωτικότητα·

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 PII12 - Πολιτική διαχείρισης ιδιωτικότητας εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών·

12.13 PII13 - Πολιτική διεθνών διαβιβάσεων PII·

12.14 PII14 - Πολιτική ασφάλειας και ελέγχου πρόσβασης PII·

12.15 PII15 - Πολιτική διαχείρισης περιστατικών και παραβιάσεων PII·

12.16 PII17 - Πολιτική διαχείρισης τεκμηριωμένων πληροφοριών και τεκμηρίων PIMS·

12.17 PII18 - Πολιτική παρακολούθησης, ελέγχου και βελτίωσης PIMS.

13. Πρότυπα και πλαίσια αναφοράς

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].