					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: PII14					Τίτλος εγγράφου: **Πολιτική ασφάλειας και ελέγχου πρόσβασης PII**							
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 6.1.3; Clause 8.1	Both	Primary	Σχεδιασμός και λειτουργία ελέγχων ασφάλειας PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Τεκμήρια, παρακολούθηση και διορθωτικά μέτρα
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Ταυτότητα και δικαιώματα πρόσβασης για επεξεργασία PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Προστασία τερματικών σημείων και ασφαλής αυθεντικοποίηση
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Καταγραφή και κρυπτογραφική προστασία
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Ασφάλεια εφαρμογών και ασφαλής αρχιτεκτονική
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Προστασία και ανασκόπηση αρχείων
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Ασφάλεια, λογοδοσία και έλεγχοι εκτελούντων την επεξεργασία
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Ενσωμάτωση ελέγχων ISMS
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Καθοδήγηση υλοποίησης ελέγχων ασφάλειας
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Αρχές ασφάλειας πληροφοριών και

				συμμόρφωσης με την ιδιωτικότητα
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Έλεγχοι ασφάλειας για την προστασία PII

1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική καθορίζει τις ειδικές για PII απαιτήσεις ασφάλειας και ελέγχου πρόσβασης για συστήματα, εφαρμογές, υπηρεσίες, συσκευές, περιβάλλοντα νέφους και επιχειρησιακές διαδικασίες που αποθηκεύουν, μεταδίδουν, επεξεργάζονται, προσπελάζουν, διαχειρίζονται ή προστατεύουν PII.

1.2 Η παρούσα πολιτική εφαρμόζεται σε πλαίσια υπευθύνου επεξεργασίας, από κοινού υπευθύνου επεξεργασίας, εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας, όπου ο οργανισμός καθορίζει, λειτουργεί, υποστηρίζει ή βασίζεται σε ελέγχους ασφάλειας για την επεξεργασία PII.

1.3 Η παρούσα πολιτική καλύπτει τους ακόλουθους τομείς ελέγχων ασφάλειας PII:

1.3.1 βασική γραμμή ασφάλειας PII και ενσωμάτωση με υφιστάμενες πολιτικές ασφάλειας πληροφοριών·

1.3.2 έλεγχο πρόσβασης·

1.3.3 αυθεντικοποίηση·

1.3.4 προνομιούχα πρόσβαση·

1.3.5 κρυπτογράφηση και ασφαλή αποθήκευση·

1.3.6 καταγραφή και παρακολούθηση·

1.3.7 ασφαλή διαμόρφωση και διαχείριση ευπαθειών·

1.3.8 ελέγχους πρόσβασης τερματικών σημείων και περιβάλλοντος νέφους·

1.3.9 σύνδεση τεκμηρίων μέσω REG02, REG08, REG10 και REG12.

1.4 Η παρούσα πολιτική δεν αντικαθιστά πλήρες σύστημα διαχείρισης ασφάλειας πληροφοριών, πολιτική ασφάλειας δικτύου, πολιτική ασφαλούς ανάπτυξης, πολιτική αντιγράφων ασφαλείας, πολιτική τερματικών σημείων, πολιτική ασφάλειας νέφους, κρυπτογραφικό πρότυπο, διαδικασία διαχείρισης ευπαθειών ή διαδικασία απόκρισης σε περιστατικά. Όπου οι πολιτικές αυτές ήδη υπάρχουν, η παρούσα πολιτική καθορίζει τη σύνδεση και τις απαιτήσεις τεκμηρίων ειδικά για PII που απαιτούνται για τη διασφάλιση PIMS.

1.5 Η παρούσα πολιτική δεν επαναλαμβάνει:

1.5.1 την απογραφή επεξεργασίας PII και την κυριότητα της νομικής βάσης στο PII03·

1.5.2 τη μεθοδολογία κινδύνου ιδιωτικότητας και DPIA στο PII07·

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

1.5.4 τους κανόνες συλλογής, χρήσης, κοινολόγησης και κοινοχρησίας στο PII09·

1.5.5 την εκτέλεση διατήρησης, διαγραφής και διάθεσης στο PII10·

1.5.6 τη διακυβέρνηση κύκλου ζωής εκτελούντων την επεξεργασία στο PII12·

1.5.7 τους ελέγχους μηχανισμών διεθνών διαβιβάσεων στο PII13·

1.5.8 τη ροή εργασίας περιστατικών και παραβιάσεων στο PII15·

1.5.9 τη διακυβέρνηση τεκμηριωμένων πληροφοριών στο PII17·

1.5.10 τη διακυβέρνηση παρακολούθησης, ελέγχου και βελτίωσης PIMS στο PII18.

1.6 Για την παρούσα πολιτική, τα επιχειρησιακά αρχεία καταγραφής, τα αποτελέσματα εργαλείων ασφάλειας, οι εξαγωγές ανασκοπήσεων πρόσβασης, οι αναφορές ευπαθειών και τα τεκμήρια διαμόρφωσης αποτελούν πηγές τεκμηρίων που επισυνάπτονται, συνοψίζονται ή παραπέμπονται στα κανονικά αντικείμενα τεκμηρίων. Δεν αποτελούν χωριστά μητρώα PIMS.

2. Σκοπός

2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίσει ότι το PII προστατεύεται με κατάλληλους, ευθυγραμμισμένους με τον κίνδυνο και ελέγξιμους ελέγχους ασφάλειας και πρόσβασης καθ' όλη τη διάρκεια της επεξεργασίας.

2.2 Η παρούσα πολιτική επιτρέπει στον οργανισμό να αποδεικνύει ότι οι έλεγχοι ασφάλειας PII σχεδιάζονται, υλοποιούνται, ανασκοπούνται, παρακολουθούνται και βελτιώνονται μέσω REG02, REG08, REG10 και REG12, χωρίς δημιουργία διπλών μητρώων ασφάλειας ή αντικατάσταση υφιστάμενων πολιτικών ασφάλειας πληροφοριών.

3. Στόχοι

3.1 Οι στόχοι της παρούσας πολιτικής είναι να:

3.1.1 καθορίζει βασική γραμμή ελέγχου πρόσβασης PII για συστήματα και δραστηριότητες επεξεργασίας·

3.1.2 διασφαλίζει ότι οι έλεγχοι αυθεντικοποίησης είναι κατάλληλοι για την ευαισθησία και το πλαίσιο πρόσβασης του PII·

3.1.3 καθορίζει απαιτήσεις ανασκόπησης για προνομιούχα και συνήθη πρόσβαση σε PII·

3.1.4 καθορίζει προσδοκίες κρυπτογράφησης και ασφαλούς αποθήκευσης για PII σε αποθήκευση, σε μεταφορά και σε σχετικά πλαίσια περιβάλλοντος νέφους ή τερματικών σημείων·

3.1.5 καθορίζει προσδοκίες καταγραφής και παρακολούθησης για την πρόσβαση σε PII, τις αλλαγές σε PII και τη διαχείριση PII·

3.1.6 καθορίζει απαιτήσεις τεκμηρίων ασφαλούς διαμόρφωσης και ευπαθειών για συστήματα που επεξεργάζονται PII·

3.1.7 καθορίζει προσδοκίες για τερματικά σημεία και πρόσβαση σε περιβάλλον νέφους, χωρίς δημιουργία πλήρους πολιτικής τερματικών σημείων ή ασφάλειας νέφους·

3.1.8 συνδέει ύποπτα περιστατικά ασφάλειας PII με REG10, χωρίς επανάληψη της ροής εργασίας περιστατικών·

3.1.9 ενσωματώνεται με υφιστάμενες πολιτικές ασφάλειας πληροφοριών όπου είναι διαθέσιμες·

3.1.10 διατηρεί τεκμήρια έτοιμα για έλεγχο χρησιμοποιώντας μόνο REG02, REG08, REG10 και REG12.

4. Δηλώσεις πολιτικής

4.1 Βασική γραμμή ασφάλειας PII και ενσωμάτωση ISMS

4.1.1 [Both] Ο Information Security Lead πρέπει να καθορίζει τη βασική γραμμή ασφάλειας PII για κάθε σύστημα ή υπηρεσία που επεξεργάζεται PII στο REG12 πριν το σύστημα ή η υπηρεσία τεθεί σε παραγωγική λειτουργία ή υποστεί ουσιώδη αλλαγή.

4.1.2 [Both] Ο System Owner / Application Owner πρέπει να καταγράφει στο REG12 τη θέση των τεκμηρίων του υλοποιημένου ελέγχου ασφάλειας PII πριν βασιστεί σε υφιστάμενο έλεγχο ασφάλειας πληροφοριών για διασφάλιση PIMS.

4.1.3 [Controller] Ο Process Owner / Business Owner πρέπει να προσδιορίζει την ευαισθησία του PII, το πλαίσιο επεξεργασίας και την ανάγκη πρόσβασης στο REG02 πριν ζητήσει νέα ή ουσιωδώς τροποποιημένη πρόσβαση σε PII.

4.1.4 [Processor] Ο Vendor / Procurement Owner πρέπει να καταγράφει τις εντολές ασφάλειας πελάτη, τα όρια ευθύνης του πελάτη και τις δεσμεύσεις ασφάλειας του εκτελούντος την επεξεργασία στο REG08 πριν αρχίσει ή αλλάξει ουσιωδώς η πρόσβαση του εκτελούντος την επεξεργασία σε PII πελάτη.

4.1.5 [Both] Ο Privacy Lead / PIMS Manager πρέπει να επαληθεύει ότι τα τεκμήρια ασφάλειας PII συνδέονται με REG02, REG08, REG10 ή REG12 πριν αποδεχθεί τη δραστηριότητα επεξεργασίας ως ελέγξιμη στο πλαίσιο PIMS.

4.2 Βασική γραμμή ελέγχου πρόσβασης

4.2.1 [Both] Ο System Owner / Application Owner πρέπει να περιορίζει την πρόσβαση σε PII σε εγκεκριμένους ρόλους και εξουσιοδοτημένους χρήστες που έχουν καταγραφεί ή είναι ιχνηλάσιμοι στο REG02 ή REG12 πριν ενεργοποιηθεί η πρόσβαση.

4.2.2 [Both] Ο Process Owner / Business Owner πρέπει να εγκρίνει τον επιχειρησιακό σκοπό της πρόσβασης σε PII στο REG02 ή REG12 πριν ο System Owner / Application Owner χορηγήσει την πρόσβαση.

4.2.3 [Both] Ο System Owner / Application Owner πρέπει να ανασκοπεί την πρόσβαση χρηστών σε συστήματα που επεξεργάζονται PII υψηλού αντικτύπου ή ευαίσθητο PII τουλάχιστον ανά τρίμηνο και να καταγράφει το αποτέλεσμα της ανασκόπησης στο REG12.

4.2.4 [Both] Ο System Owner / Application Owner πρέπει να ανασκοπεί την πρόσβαση χρηστών σε άλλα συστήματα που επεξεργάζονται PII τουλάχιστον ετησίως και να καταγράφει το αποτέλεσμα της ανασκόπησης στο REG12.

4.2.5 [Both] Ο System Owner / Application Owner πρέπει να αφαιρεί ή να τροποποιεί την πρόσβαση σε PII στο REG12 εντός μίας εργάσιμης ημέρας μετά από αλλαγή ρόλου, λύση απασχόλησης, ολοκλήρωση σύμβασης ή όταν η πρόσβαση δεν απαιτείται πλέον.

4.2.6 [Processor] Ο Vendor / Procurement Owner πρέπει να επιβεβαιώνει στο REG08 ότι η πρόσβαση του εκτελούντος την επεξεργασία σε PII πελάτη περιορίζεται στις τεκμηριωμένες εντολές πελάτη πριν ενεργοποιηθεί ή αλλάξει η πρόσβαση.

4.2.7 [Subprocessor] Ο Vendor / Procurement Owner πρέπει να επιβεβαιώνει στο REG08 ότι η πρόσβαση υπεργολάβου επεξεργασίας σε PII περιορίζεται σε εξουσιοδοτημένες δραστηριότητες υπεργολαβικής επεξεργασίας πριν ενεργοποιηθεί ή αλλάξει η πρόσβαση υπεργολάβου επεξεργασίας.

[... 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 [Both] Ο Information Security Lead πρέπει να καταγράφει κάθε εξαίρεση από απαίτηση ασφάλειας ή ελέγχου πρόσβασης PII στο REG12 πριν ενεργοποιηθεί η εξαίρεση.

9.1.2 [Both] Ο Data Protection Officer / Privacy Advisor πρέπει να παρέχει συμβουλή για εξαιρέσεις ασφάλειας PII υψηλότερου κινδύνου στο REG12 πριν από την έγκριση.

9.1.3 [Both] Το Top Management πρέπει να εγκρίνει εξαιρέσεις ασφάλειας PII στο REG12 πριν από την ενεργοποίηση, όταν η εξαίρεση επηρεάζει PII υψηλού αντικτύπου, ευαίσθητο PII, προνομιούχα πρόσβαση, κρυπτογράφηση, καταγραφή ή μη επιλυμένες ευπάθειες υψηλού κινδύνου.

9.1.4 [Both] Ο Information Security Lead πρέπει να καθορίζει στο REG12 τη λήξη της εξαίρεσης, τον αντισταθμιστικό έλεγχο και την ημερομηνία ανασκόπησης πριν από την έγκριση της εξαίρεσης.

9.1.5 [Both] Ο System Owner / Application Owner πρέπει να αποκαθιστά, να ανανεώνει ή να κλείνει ληγμένες εξαιρέσεις ασφάλειας PII στο REG12 εντός πέντε εργάσιμων ημερών μετά τη λήξη.

9.1.6 [Processor] Ο Vendor / Procurement Owner πρέπει να καταγράφει εξαιρέσεις ασφάλειας εκτελούντος την επεξεργασία ή υπεργολάβου επεξεργασίας που επηρεάζουν PII πελάτη στο REG08 και REG12 πριν από την αποδοχή.

10. Εφαρμογή

10.1.1 [Both] Ο Privacy Lead / PIMS Manager πρέπει να καταγράφει μη συμμορφώσεις για ελλείποντα ή ελλιπή τεκμήρια ασφάλειας PII στο REG12 εντός πέντε εργάσιμων ημερών από τον εντοπισμό.

10.1.2 [Both] Ο Information Security Lead πρέπει να αναθέτει κυριότητα αποκατάστασης για αστοχίες ελέγχων ασφάλειας PII στο REG12 εντός πέντε εργάσιμων ημερών από την επικύρωση.

10.1.3 [Both] Ο System Owner / Application Owner πρέπει να απενεργοποιεί ή να περιορίζει μη εξουσιοδοτημένη, υπερβολική ή μη υποστηριζόμενη πρόσβαση σε PII εντός μίας εργάσιμης ημέρας από την επικύρωση και να καταγράφει την ενέργεια στο REG12.

10.1.4 [Conditional] Ο Incident Response Coordinator πρέπει να συνδέει ενέργειες εφαρμογής με REG10 εντός μίας εργάσιμης ημέρας όταν το ζήτημα εφαρμογής αφορά ύποπτο ή επιβεβαιωμένο περιστατικό PII.

10.1.5 [Both] Το Top Management πρέπει να ανασκοπεί επαναλαμβανόμενες ή υψηλού κινδύνου μη συμμορφώσεις ασφάλειας PII στο REG12 πριν από την ανασκόπηση της διοίκησης.

11. Ανασκόπηση και συντήρηση

11.1.1 [All] Ο Privacy Lead / PIMS Manager πρέπει να ανασκοπεί την παρούσα πολιτική με τον Information Security Lead τουλάχιστον ετησίως και να καταγράφει το αποτέλεσμα της ανασκόπησης στο REG12.

11.1.2 [Both] Ο Information Security Lead πρέπει να ανασκοπεί τη βασική γραμμή ασφάλειας PII στο REG12 εντός 30 ημερών μετά από ουσιώδη τεχνολογική αλλαγή, αλλαγή απειλής, ελέγχου, περιστατικού ή κανονιστική αλλαγή που επηρεάζει την ασφάλεια PII.

11.1.3 [Both] Ο System Owner / Application Owner πρέπει να επικαιροποιεί τα τεκμήρια ασφάλειας PII σε επίπεδο συστήματος στο REG12 εντός 30 ημερών μετά από ουσιώδη αλλαγή αρχιτεκτονικής, πρόσβασης, διαμόρφωσης, ευπάθειας ή καταγραφής.

11.1.4 [Processor] Ο Vendor / Procurement Owner πρέπει να ανασκοπεί τα τεκμήρια ευθύνης ασφάλειας PII εκτελούντων την επεξεργασία και υπεργολάβων επεξεργασίας στο REG08 εντός 30 ημερών μετά από ουσιώδη αλλαγή υπηρεσίας, εντολής πελάτη ή υπεργολάβου επεξεργασίας.

11.1.5 [All] Ο Internal Audit / Compliance Reviewer πρέπει να επαληθεύει τα τεκμήρια ανασκόπησης πολιτικής και επιλεγμένα τεκμήρια ελέγχων ασφάλειας PII στο REG12 σύμφωνα με το εγκεκριμένο σχέδιο ελέγχων.

12. Συναφείς πολιτικές

12.1 Η παρούσα πολιτική πρέπει να διαβάζεται σε συνδυασμό με:

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 PII07 - Πολιτική αξιολόγησης κινδύνου ιδιωτικότητας και DPIA·

12.6 PII08 - Πολιτική προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού·

12.7 PII09 - Πολιτική συλλογής, χρήσης, κοινολόγησης και κοινοχρησίας PII·

12.8 PII10 - Πολιτική διατήρησης, διαγραφής και διάθεσης PII·

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

12.10 PII13 - Πολιτική διεθνών διαβιβάσεων PII·

12.11 PII15 - Πολιτική διαχείρισης περιστατικών και παραβιάσεων PII·

12.12 PII16 - Πολιτική εκπαίδευσης, ευαισθητοποίησης και επάρκειας σε θέματα ιδιωτικότητας·

12.13 PII17 - Πολιτική διαχείρισης τεκμηριωμένων πληροφοριών και τεκμηρίων PIMS·

12.14 PII18 - Πολιτική παρακολούθησης, ελέγχου και βελτίωσης PIMS.

13. Πρότυπα και πλαίσια αναφοράς

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].