Ειδικός Κανονισμός Πιστοποίησης Συστημάτων Διαχείρισης Πιστοποίηση Συστημάτων Διαχείρισης Πληροφοριών Ιδιωτικότητας (ΣΔΠΙ) κατά ΕΛΟΤ ΕΝ ISO/IEC 27701:2021

1. Ειδικές Προδιαγραφές Πιστοποίησης ΣΔΠΙ

Η αρχική πιστοποίηση, όπως επίσης και οι επιτηρήσεις της πιστοποίησης και η επαναπιστοποίηση, **Συστημάτων Διαχείρισης Πληροφοριών Ιδιωτικότητας** (**ΣΔΠΙ**) κατά **ΕΛΟΤ ΕΝ ISO/IEC 27701:2021** βασίζονται στις γενικές απαιτήσεις, όπως αυτές αναγράφονται στο Γενικό Κανονισμό Πιστοποίησης Συστημάτων Διαχείρισης (**ΓΚΠΣΔ**), και πιο συγκεκριμένα σε αυτές των κάτωθι:

- **ΕΛΟΤ ISO/IEC 27001:2013** «Τεχνολογία πληροφοριών – Τεχνικές ασφάλειας – Συστήματα διαχείρισης της ασφάλειας πληροφοριών – Απαιτήσεις»
- **ΕΛΟΤ ISO/IEC 27002:2013** «Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κώδικας πρακτικής για τους ελέγχους ασφάλειας των πληροφοριών»
- **ISO/IEC 27006:2015** «Ασφάλεια πληροφοριών - Τεχνικές ασφάλειας - Απαιτήσεις για Φορείς που διενεργούν επιθεωρήσεις και πιστοποιήσεις σε Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών»
- **ISO/IEC 27006:2015/Amd.1:2020** «Ασφάλεια πληροφοριών - Τεχνικές ασφάλειας - Απαιτήσεις για Φορείς που διενεργούν επιθεωρήσεις και πιστοποιήσεις σε Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Τροπολογία 1»
- **ISO/IEC TS 27006-2:2021** «Απαιτήσεις για Φορείς που διενεργούν επιθεωρήσεις και πιστοποιήσεις σε Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών – Μέρος 2: Συστήματα Διαχείρισης Πληροφοριών Ιδιωτικότητας»
- **ΕΛΟΤ ΕΝ ISO/IEC 27701:2021** «Τεχνικές ασφάλειας - Επέκταση σε ISO/IEC 27001 και ISO/IEC 27002 για διαχείριση πληροφοριών απορρήτου - Απαιτήσεις και οδηγίες»

2. Περιγραφή της Πιστοποίησης ΣΔΠΙ

Η πιστοποίηση του ΣΔΠΙ ενός οργανισμού κατά ΕΛΟΤ ΕΝ ISO/IEC 27701:2021 καθορίζεται από τις προδιαγραφές του Εγχειριδίου Ποιότητας, του Γενικού Κανονισμού Πιστοποίησης ΣΔ και του παρόντος, των διαδικασιών ποιότητας και οδηγιών εργασίας που έχει δημιουργήσει και εναρμονιστεί ο Φορέας Πιστοποίησης UCERT, και που συμμορφώνονται με τις ανωτέρω απαιτήσεις.

Στόχος της πιστοποίησης αυτής είναι να εκτιμήσει την πλήρη εναρμόνιση του οργανισμού στη σύνθεση, την εκτέλεση, τη συντήρηση και τη συνεχή βελτίωση ενός Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας. Η συμμόρφωση αυτή έγκειται σε απόδειξη:

- της ικανότητας και συνέπειας κατά τη διατήρηση και τη συνεχή βελτίωση ενός Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας,
- την αξιολόγηση και την αντιμετώπιση των κινδύνων για τις **Πληροφορίες Προσωπικής Ταυτοποίησης-ΠΠΤ** (***Personally Identifiable Information-PII***).

Τονίζεται ότι το πρότυπο ΕΛΟΤ ΕΝ ISO/IEC 27701:2021 υλοποιείται σε οποιονδήποτε οργανισμό, ανεξαρτήτως της έκτασης και της χρήσης του, όπως και των προϊόντων ή/και υπηρεσιών που παράγει ή/και παρέχει. Επιβάλλεται δε η ύπαρξη **ΣΔΑΠ** το οποίο συμμορφώνεται με τις επιπρόσθετες προδιαγραφές του προτύπου που αφορούν την προστασία των ΠΠΤ (**ΟΣΔ**) ή υποστηρίζει το ΣΔΠΙ.

Το ISO/IEC 27701 είναι το πλέον κατάλληλο διεθνές πρότυπο που αναγνωρίζεται παγκοσμίως για τη διαχείριση κινδύνων για τις Πληροφορίες Προσωπικής Ταυτοποίησης που διατηρούνται από μια εταιρία. Η πιστοποίηση κατά το πρότυπο ISO/IEC 27701 δίνει στον Οργανισμό την δυνατότητα να αποδείξει στους πελάτες του αλλά και σε άλλα ενδιαφερόμενα μέρη ότι διαχειρίζεται με δέουσα εμπιστευτικότητα τις Πληροφορίες Προσωπικής Ταυτοποίησης. Η τρέχουσα έκδοση του προτύπου διαθέτει ένα σύνολο τυποποιημένων απαιτήσεων για ένα ολοκληρωμένο ΣΔΠΙ. Το πρότυπο

ενστερνίζεται μια προσέγγιση βασισμένη στη διαδικασία για τη σύνθεση, την εκτέλεση, τη λειτουργία, την επιτήρηση, τη συντήρηση και τη βελτίωση του ΣΔΠΙ κάθε οργανισμού.

3. Τύπος Πιστοποιητικού

Το πιστοποιητικό που εκδίδεται από τον Φορέα Πιστοποίησης UCERT αναφέρεται στην πιστοποίηση **ΣΔΠΙ** κατά ΕΛΟΤ ΕΝ ISO/IEC 27701:2021.

4. Διαδικασία Πιστοποίησης ΣΔΠΙ

Ο Φορέας Πιστοποίησης UCERT αναλαμβάνει να εκτιμήσει την εναρμόνιση του **ΣΔΠΙ** ενός οργανισμού με τις προδιαγραφές του διεθνούς προτύπου **ΕΛΟΤ ΕΝ ISO/IEC 27701:2021**, με τη συνεισφορά των μελών του προσωπικού του Φορέα που συμμετέχουν σε αυτή τη διαδικασία (των οποίων οι δεξιότητες ικανοποιούν τις απαιτήσεις της ισχύουσας έκδοσης του προτύπου ISO/IEC TS 27006-2 και της διαδικασίας **Δ36**) και των μελών του Μητρώου Επιθεωρητών/Εμπειρογνωμόνων Πιστοποίησης ΣΔ.

Ο Φορέας Πιστοποίησης UCERT δεν παρέχει υπηρεσίες συμβουλευτικής ΣΔ σχετικά με το ΣΔΠΙ, όπως, π.χ., υπηρεσίες ως εξωτερικός υπεύθυνος προστασίας δεδομένων, ανασκοπήσεις διεργασιών ή ανασκοπήσεις προστασίας δεδομένων. Η οργάνωση και συμμετοχή ως εισηγητής σε εκπαιδευτικά μαθήματα που σχετίζονται με συστήματα διαχείρισης ασφάλειας προσωπικών πληροφοριών δεν θεωρείται υπηρεσία συμβουλευτικής ούτε θεωρείται πιθανή σύγκρουση συμφερόντων, υπό την προϋπόθεση ότι εφαρμόζονται οι διατάξεις της παραγράφου 5.2.1.a του ISO/IEC 27006:2015.

4.1. Στάδια Επιθεώρησης ΣΔΠΙ

Η διαδικασία της επιθεώρησης ΣΔΠΙ αποτελείται από δύο στάδια, τα οποία διενεργούνται στις εγκαταστάσεις του πελάτη, ύστερα από την ενημέρωσή του για τα αντίστοιχα σχέδια επιθεώρησης, και συμπεριλαμβάνει τη διαπίστωση της συμμόρφωσης και με τις απαιτήσεις του ISO/IEC 27001.

4.2. Επιθεωρητές ΣΔΠΙ

Το Μητρώο Επιθεωρητών/Εμπειρογνωμόνων Πιστοποίησης ΣΔ του Φορέα Πιστοποίησης UCERT αποτελείται από μέλη κατάλληλα να ανταποκριθούν στις προϋποθέσεις της επιθεώρησης ενός ΣΔΠΙ.

Τα μέλη του Μητρώου είναι πεπειραμένοι επιθεωρητές ΣΔΠΙ κατά ΕΛΟΤ ΕΝ ISO/IEC 27701:2021 και η επάρκειά τους αναλύεται στη διαδικασία **Δ36-6**.

Ο Επικεφαλής Επιθεωρητής διεξάγει και τα δύο στάδια της επιθεώρησης, τόσο κατά την αρχική πιστοποίηση ενός ΣΔΠΙ, όσο και κατά την επιτήρηση της πιστοποίησης και επαναπιστοποίησή του.

Η συνδρομή Τεχνικών Εμπειρογνωμόνων (χωρίς την προϋπόθεση της ιδιότητας του επιθεωρητή) θεωρείται αναγκαία όταν το πεδίο εφαρμογής της πιστοποίησης του ΣΔΠΙ δεν καλύπτεται από τα προσόντα όλων των μελών της Ομάδας Επιθεώρησης ΣΔ.

Στις υποχρεώσεις των Επιθεωρητών συμπεριλαμβάνονται και τα παρακάτω:

- Συνεχή ενημέρωση και επιμόρφωση αναφορικά με τις μεταβολές στη νομοθεσία που διέπει την πιστοποίηση ΣΔΠΙ, αλλά και τη λειτουργία και τα αγαθά των υπό πιστοποίηση ΣΔΠΙ των οργανισμών
- Μη ύπαρξη σχέσης (οικονομικής, εμπορικής ή οποιουδήποτε άλλου είδους) με τον οργανισμό του οποίου το ΣΔΠΙ επιθεωρείται κατά τα δύο (2) τελευταία έτη

Ο Φορέας ενημερώνεται για τις μεταβολές στη νομοθεσία που σχετίζεται με την πιστοποίηση και υποχρεούται να ανασκοπεί τα έγγραφα του ΣΔ που υλοποιεί και να ενημερώνει ή και εκπαιδεύει κατάλληλα τα μέλη του Μητρώου Επιθεωρητών.

4.3.Διεξαγωγή Επιθεώρησης ΣΔΠΙ

Μετά την έγκριση της αίτησης αρχικής πιστοποίησης του ΣΔΠΙ από τον πελάτη, τον προγραμματισμό της διάρκειας της επιθεώρησης από τον Υπεύθυνο Πιστοποίησης ΣΔ και την θετική αξιολόγηση της επάρκειας της προσκομισθείσας από τον πελάτη τεκμηρίωσης από τον Επικεφαλής Επιθεωρητή, ο Επικεφαλής Επιθεωρητής αναπτύσσει το κατάλληλο για τη συγκεκριμένη χρονική διάρκεια Σχέδιο Επιθεώρησης. Τονίζεται ότι η διάρκεια αυτή ενδέχεται να διαφοροποιηθεί βάση των συνθήκων και των ευρημάτων της επιθεώρησης. Επίσης, το Σχέδιο Επιθεώρησης λαμβάνει υπόψη όχι μόνον τους ελέγχους του ΣΔΠΙ, αλλά και του ΣΔΑΠ.

Σε περίπτωση ύπαρξης περισσότερων της μίας εγκαταστάσεων, ο Φορέας μπορεί να επιλέξει ποιες απ' αυτές θα επιθεωρηθούν, εκτός αυτής που θεωρείται κεντρική (από όπου ασκείται η διοίκηση). Η πιστοποίηση του ΣΔΠΙ ενός τέτοιου οργανισμού αφορά τη εφαρμογή στο σύνολο του οργανισμού, πλην των εγκαταστάσεων που σύμφωνα με την αίτησή του θα εξαιρεθούν της πιστοποίησης.

Η επιθεώρηση διενεργείται από την ορισμένη Ομάδα Επιθεώρησης ΣΔΠΙ με γνώμονα τις προδιαγραφές του Ποιότητας, του Γενικού Κανονισμού Πιστοποίησης ΣΔ (ΓΚΠΣΔ) και του παρόντος, των διαδικασιών ποιότητας και οδηγιών εργασίας, καθώς και με χρήση των κατάλληλων εντύπων που απαιτούνται.

Διάρθρωση της Επιθεώρησης ΣΔΠΙ

Η επιθεώρηση που διενεργείται είναι διαρθρωμένη όμοια με το πρότυπο ΕΛΟΤ EN ISO/IEC 27701:2021. Επιγραμματικά στον παρακάτω πίνακα αναφέρονται οι απαιτήσεις του προτύπου με τις οποίες ο οργανισμός πρέπει να εναρμονίζεται. Σημειώνεται ότι όσα επισημαίνονται με αστερίσκο (*) αφορούν προδιαγραφές ακριβώς όμοιες με του προτύπου ΕΛΟΤ EN ISO/IEC 27001:2013 (σε παρένθεση η αντίστοιχη παράγραφος), ενώ όλα τα υπόλοιπα αφορούν προδιαγραφές τουλάχιστον αυτές του προτύπου ΕΛΟΤ EN ISO/IEC 27001:2013 (σε παρένθεση η αντίστοιχη παράγραφος), δηλαδή επαυξάνονται με προδιαγραφές που σχετίζονται αποκλειστικά με την προστασία των ΠΠΤ.

§	Απαιτήσεις
5.2. **(4.)**	**Πλαίσιο Λειτουργίας του Οργανισμού** 1. Κατανόηση του οργανισμού και του πλαισίου λειτουργίας του 2. Κατανόηση των αναγκών και των προσδοκιών των ενδιαφερόμενων μερών 3. Καθορισμός του πεδίου εφαρμογής του Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας 4. Σύστημα Διαχείρισης Πληροφοριών Ιδιωτικότητας (και διεργασίες του)
5.3.* **(5.)**	**Ηγεσία** 1. Ηγεσία και δέσμευση 2. Πολιτική 3. Ρόλοι, υπευθυνότητες και αρμοδιότητες εντός του οργανισμού
5.4. **(6.)**	**Σχεδιασμός** 1. Ενέργειες για την αντιμετώπιση απειλών και την αξιοποίηση ευκαιριών 1.1. Γενικά 1.2. Αξιολόγηση κινδύνων σχετικών με την ασφάλεια και το απόρρητο πληροφοριών 1.3. Αντιμετώπιση κινδύνων σχετικών με την ασφάλεια και το απόρρητο πληροφοριών 2. Στόχοι ασφάλειας και απορρήτου πληροφοριών και σχεδιασμός για την επίτευξή τους
5.5.* **(7.)**	**Υποστήριξη** 1. Πόροι 2. Επαγγελματική επάρκεια 3. Ευαισθητοποίηση 4. Επικοινωνία 5. Τεκμηριωμένες πληροφορίες 5.1. Γενικά 5.2. Δημιουργία και ενημέρωση 5.3. Έλεγχος των τεκμηριωμένων πληροφοριών

§	Απαιτήσεις
5.6.* (8.)	**Λειτουργία** 1. Σχεδιασμός και έλεγχος της λειτουργίας (διεργασιών) 2. Αξιολόγηση κινδύνων σχετικών με την ασφάλεια και το απόρρητο πληροφοριών 3. Αντιμετώπιση κινδύνων σχετικών με την ασφάλεια και το απόρρητο πληροφοριών
5.7.* (9.)	**Αξιολόγηση Επιδόσεων** 1. Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση 2. Εσωτερική επιθεώρηση 2.1. Γενικά 2.2. Πρόγραμμα εσωτερικής επιθεώρησης 3. Ανασκόπηση από τη Διοίκηση 3.1. Γενικά 3.2. Εισερχόμενα της ανασκόπησης από τη Διοίκηση 3.3. Αποτελέσματα της ανασκόπησης από τη Διοίκηση
5.8.* (10.)	**Βελτίωση** 1. Μη συμμόρφωση και διορθωτικές ενέργειες 2. Συνεχής βελτίωση
6.2. (A.5.)	**Πολιτικές Ασφάλειας και Απορρήτου Πληροφοριών** 1. Διαχείριση κατευθύνσεων για την ασφάλεια και το απόρρητο πληροφοριών 1.1. Πολιτικές ασφάλειας και απορρήτου πληροφοριών 1.2. Ανασκόπηση πολιτικών ασφάλειας και απορρήτου πληροφοριών
6.3. (A.6.)	**Οργάνωση Ασφάλειας και Απορρήτου Πληροφοριών** 1. Εσωτερική οργάνωση 1.1. Ρόλοι και αρμοδιότητες ασφάλειας και απορρήτου πληροφοριών 1.2. Καθορισμός καθηκόντων 1.3. Επαφή με τις αρχές 1.4. Επαφή με ειδικές ομάδες ενδιαφέροντος 1.5. Ασφάλεια και απόρρητο πληροφοριών στη διαχείριση έργου 2. Τηλε-εργασία και απομακρυσμένη πρόσβαση 2.1. Πολιτική κινητών συσκευών 2.2. Τηλε-εργασία
6.4. (A.7.)	**Ασφάλεια Ανθρώπινου Δυναμικού** 1. Πριν την πρόσληψη 1.1. Διαλογή (Screening) 1.2. Όροι και συνθήκες εργασίας 2. Κατά τη διάρκεια της εργασίας 2.1. Ευθύνες της διοίκησης 2.2. Επίγνωση, ενημέρωση και επιμόρφωση για την ασφάλεια και το απόρρητο πληροφοριών 2.3. Πειθαρχικές διαδικασίες 3. Απόλυση/Αποχώρηση προσωπικού 3.1. Αρμοδιότητες λήξης ή αλλαγής εργασίας
6.5. (A.8.)	**Διαχείριση Πόρων** 1. Ευθύνη για τους πόρους 1.1. Λίστα πόρων 1.2. Ιδιοκτησία πόρων 1.3. Αποδεκτή χρήση πόρων 1.4. Επιστροφή πόρων 2. Διαβάθμιση πληροφορίας 2.1. Κανόνες διαβάθμισης 2.2. Επισήμανση και χειρισμός πληροφοριών 2.3. Χειρισμός πόρων 3. Διαχείριση μέσων αποθήκευσης 3.1. Διαχείριση φορητών μέσων αποθήκευσης 3.2. Καταστροφή μέσων αποθήκευσης 3.3. Διακινούμενα φυσικά μέσα

§	Απαιτήσεις
6.6. (A.9.)	**Έλεγχος Πρόσβασης** 1. Απαιτήσεις ελέγχου πρόσβασης 1.1. Πολιτική ελέγχου πρόσβασης 1.2. Πρόσβαση στο δίκτυο 2. Διαχείριση πρόσβασης χρηστών 2.1. Εγγραφή/Διαγραφή χρηστών 2.2. Παροχή πρόσβασης χρηστών 2.3. Διαχείριση προνομιακών δικαιωμάτων 2.4. Διαχείριση πληροφοριών αυθεντικοποίησης 2.5. Ανασκόπηση δικαιωμάτων πρόσβασης χρηστών 2.6. Αφαίρεση/Τροποποίηση δικαιωμάτων πρόσβασης 3. Αρμοδιότητες χρηστών 3.1. Χρήση μυστικής πληροφορίας αυθεντικοποίησης 4. Έλεγχος πρόσβασης σε εφαρμογές και συστήματα 4.1. Περιορισμός πρόσβασης στην πληροφορία 4.2. Διαδικασίες ασφαλούς σύνδεσης 4.3. Διαχείριση συνθηματικών συστήματος 4.4. Χρήση εργαλείων συστήματος 4.5. Έλεγχος πρόσβασης στον πηγαίο κώδικα των εφαρμογών
6.7. (A.10.)	**Κρυπτογραφία** 1. Κρυπτογραφικά εργαλεία 1.1. Πολιτική χρήσης κρυπτογραφικών εργαλείων 1.2. Διαχείριση κλειδιών
6.8. (A.11.)	**Φυσική Ασφάλεια Χώρων** 1. Ασφαλείς περιοχές 1.1. Περίμετρος φυσικής ασφάλειας 1.2. Έλεγχος φυσικής ασφάλειας 1.3. Προστασία γραφείων-δωματίων και λοιπών χώρων 1.4. Προστασία από εξωτερικές και περιβαλλοντικές απειλές 1.5. Εργασίες σε ασφαλισμένες περιοχές 1.6. Περιοχές φόρτωσης/παράδοσης 2. Εξοπλισμός 2.1. Εγκατάσταση και προστασία εξοπλισμού 2.2. Υποστηρικτικά δίκτυα 2.3. Ασφάλεια καλωδιώσεων 2.4. Συντήρηση εξοπλισμού 2.5. Αφαίρεση πόρων 2.6. Ασφάλεια εξοπλισμού εκτός εγκαταστάσεων 2.7. Ασφαλής καταστροφή ή επαναχρησιμοποίηση εξοπλισμού 2.8. Μη παρακολουθούμενος εξοπλισμός 2.9. Πολιτική «καθαρού γραφείου»/«καθαρής οθόνης
6.9. (A.12.)	**Ασφάλεια Λειτουργιών** 1. Επιχειρησιακές διαδικασίες και αρμοδιότητες 1.1. Τεκμηρίωση διαδικασιών 1.2. Διαχείριση αλλαγών 1.3. Διαχείριση πόρων 1.4. Διαχωρισμός διαδικασιών ανάπτυξης, δοκιμής και λειτουργίας 2. Προστασία από κακόβουλο λογισμικό 2.1. Προστασία από κακόβουλο κώδικα 3. Αντίγραφα ασφάλειας 3.1. Αντίγραφα ασφάλειας πληροφοριών 4. Καταγραφή και παρακολούθηση 4.1. Καταγραφή ενεργειών χρηστών 4.2. Προστασία αρχείων καταγραφής 4.3. Αρχεία καταγραφής Διαχειριστών 4.4. Συγχρονισμός ρολογιών

§	Απαιτήσεις
	5. Έλεγχος επιχειρησιακού λογισμικού 5.1. Εγκατάσταση λογισμικού στα επιχειρησιακά συστήματα 6. Διαχείριση τεχνικών αδυναμιών 6.1. Διαχείριση τεχνικών αδυναμιών 6.2. Περιορισμοί στην εγκατάσταση λογισμικού 7. Παράμετροι επιθεώρησης πληροφοριακών συστημάτων 7.1. Μέτρα επιθεώρησης
6.10. (Α.13.)	**Ασφάλεια Επικοινωνιών** 1. Διαχείριση ασφάλειας δικτύου 1.1. Έλεγχοι δικτύου 1.2. Ασφάλεια δικτυακών υπηρεσιών 1.3. Διαχωρισμός δικτύων 2. Ανταλλαγή πληροφορίας 2.1. Πολιτικές και διαδικασίες ανταλλαγής πληροφοριών 2.2. Συμφωνίες ανταλλαγής πληροφοριών 2.3. Ηλεκτρονική ανταλλαγή μηνυμάτων 2.4. Συμφωνίες εμπιστευτικότητας
6.11. (Α.14.)	**Προμήθεια, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων** 1. Απαιτήσεις ασφάλειας πληροφοριακών συστημάτων 1.1. Ανάλυση και προσδιορισμός απαιτήσεων ασφάλειας και απορρήτου πληροφοριών 1.2. Προστασία υπηρεσιών εφαρμογών σε δημόσια δίκτυα 1.3. Προστασία συναλλαγών 2. Ασφάλεια και απόρρητο πληροφοριών στις διαδικασίες ανάπτυξης και υποστήριξης 2.1. Πολιτική ασφαλούς ανάπτυξης 2.2. Διαδικασίες ελέγχου αλλαγών 2.3. Τεχνικός έλεγχος εφαρμογών μετά από αλλαγές σε λειτουργικές πλατφόρμες 2.4. Περιορισμοί στις αλλαγές του λογισμικού 2.5. Αρχές μηχανικής ασφαλών συστημάτων 2.6. Περιβάλλον ασφαλούς ανάπτυξης 2.7. Ανάπτυξη εφαρμογών από τρίτους 2.8. Έλεγχος ασφάλειας συστήματος 2.9. Έλεγχος αποδοχής συστήματος 3. Δεδομένα δοκιμών 3.1. Προστασία των δεδομένων ελέγχου
6.12. (Α.15.)	**Σχέσεις με Προμηθευτές** 1. Ασφάλεια και απόρρητο πληροφοριών στις σχέσεις με προμηθευτές 1.1. Πολιτική ασφάλειας και απορρήτου πληροφοριών για τη σχέση με τους προμηθευτές 1.2. Αντιμετώπιση ασφάλειας και απορρήτου πληροφοριών σε συμφωνίες με τρίτους 1.3. Εφοδιαστική αλυσίδα των Τεχνολογιών Πληροφορίας και Επικοινωνιών 2. Διαχείριση παροχής υπηρεσιών από προμηθευτές 2.1. Παρακολούθηση και ανασκόπηση υπηρεσιών από προμηθευτές 2.2. Διαχείριση αλλαγών σε υπηρεσίες τρίτων
6.13. (Α.16.)	**Διαχείριση Περιστατικών Ασφάλειας και Απορρήτου Πληροφοριών** 1. Διαχείριση περιστατικών ασφάλειας και απορρήτου πληροφοριών και βελτιώσεις 1.1. Αρμοδιότητες και διαδικασίες 1.2. Αναφορά περιστατικών ασφάλειας και απορρήτου πληροφοριών 1.3. Αναφορά αδυναμιών ασφάλειας και απορρήτου πληροφοριών 1.4. Αξιολόγηση και εκτίμηση συμβάντων ασφάλειας και απορρήτου πληροφοριών 1.5. Ανταπόκριση περιστατικών ασφάλειας και απορρήτου πληροφοριών 1.6. Μάθηση από περιστατικά ασφάλειας και απορρήτου πληροφοριών 1.7. Συλλογή πειστηρίων
6.14.* (Α.17.)	**Διαχείριση Επιχειρησιακής Συνέχειας** 1. Ασφάλεια και απόρρητο πληροφοριών για την επιχειρησιακή συνέχεια 1.1. Σχεδιασμός επιχειρησιακής συνέχειας για την ασφάλεια και το απόρρητο πληροφοριών

§	Απαιτήσεις
	1.2. Ανάπτυξη επιχειρησιακής συνέχειας για την ασφάλεια και το απόρρητο πληροφοριών 1.3. Επαλήθευση, ανασκόπηση και αξιολόγηση ασφάλειας και απορρήτου πληροφοριών για την επιχειρησιακή συνέχεια 2. Επάρκεια πληροφοριών 2.1. Διαθεσιμότητα των εγκαταστάσεων επεξεργασίας της πληροφορίας
6.15. (A.18.)	**Συμμόρφωση** 1. Συμμόρφωση με νομικές απαιτήσεις 1.1. Εντοπισμός σχετικής νομοθεσίας και απαιτήσεις συμβάσεων 1.2. Πνευματικά δικαιώματα 1.3. Προστασία αρχείων 1.4. Ιδιωτικότητα και προστασία προσωπικών πληροφοριών 1.5. Ρύθμιση κρυπτογραφικών διαδικασιών 2. Ανασκόπηση ασφάλειας και απορρήτου πληροφοριών 2.1. Ανεξάρτητος έλεγχος της ασφάλειας και του απορρήτου πληροφοριών 2.2. Συμμόρφωση με πολιτικές και προδιαγραφές ασφάλειας και απορρήτου πληροφοριών 2.3. Ανασκόπηση τεχνικής συμμόρφωσης
7.	**Πρόσθετοι έλεγχοι για ελεγκτές ΠΠΤ** 2. Προϋποθέσεις συλλογής και επεξεργασίας 2.1. Προσδιορισμός και τεκμηρίωση σκοπού 2.2. Προσδιορισμός της νόμιμης βάσης 2.3. Καθορισμός του πότε και πώς θα ληφθεί η συγκατάθεση 2.4. Λήψη και καταγραφή συγκατάθεσης 2.5. Αξιολόγηση επιπτώσεων στην ιδιωτική ζωή 2.6. Συμβάσεις με επεξεργαστές ΠΠΤ 2.7. Από κοινού επεξεργασία ΠΠΤ με ελεγκτή ΠΠΤ 2.8. Αρχεία που σχετίζονται με την επεξεργασία ΠΠΤ 3. Υποχρεώσεις προς εντολείς ΠΠΤ 3.1. Καθορισμός και εκπλήρωση υποχρεώσεων προς τους εντολείς ΠΠΤ 3.2. Προσδιορισμός πληροφοριών για εντολείς ΠΠΤ 3.3. Παροχή πληροφοριών στους εντολείς ΠΠΤ 3.4. Παροχή μηχανισμού για τροποποίηση ή ανάκληση συγκατάθεσης 3.5. Παροχή μηχανισμού αντίρρησης στην επεξεργασία ΠΠΤ 3.6. Πρόσβαση, διόρθωση ή/και διαγραφή 3.7. Υποχρεώσεις των ελεγκτών ΠΠΤ για ενημέρωση τρίτων 3.8. Παροχή αντιγράφου των ΠΠΤ που υποβάλλονται σε επεξεργασία 3.9. Χειρισμός αιτημάτων 3.10. Αυτοματοποιημένη λήψη αποφάσεων 4. Απόρρητο από το σχεδιασμό και απόρρητο εξ ορισμού 4.1. Οριακή συλλογή 4.2. Οριακή επεξεργασία 4.3. Ακρίβεια και ποιότητα 4.4. Στόχοι ελαχιστοποίησης ΠΠΤ 4.5. Αποταυτοποίηση και διαγραφή ΠΠΤ στο τέλος της επεξεργασίας 4.6. Προσωρινά αρχεία 4.7. Διατήρηση 4.8. Απόρριψη 4.9. Μετάδοση ΠΠΤ 5. Κοινή χρήση, μεταφορά και αποκάλυψη ΠΠΤ 5.1. Προσδιορισμός της βάσης για τη μεταφορά ΠΠΤ μεταξύ δικαιοδοσιών 5.2. Χώρες και διεθνείς οργανισμοί όπου μπορούν να μεταφερθούν ΠΠΤ 5.3. Αρχεία μεταφοράς ΠΠΤ 5.4. Αρχεία γνωστοποίησης ΠΠΤ σε τρίτους
8.	**Πρόσθετοι έλεγχοι για επεξεργαστές ΠΠΤ** 2. Προϋποθέσεις συλλογής και επεξεργασίας

§	Απαιτήσεις
	2.1. Συμφωνία πελάτη 2.2. Σκοποί του οργανισμού 2.3. Μάρκετινγκ και διαφημιστική χρήση 2.4. Οδηγία παράβασης 2.5. Υποχρεώσεις πελατών 2.6. Αρχεία που σχετίζονται με την επεξεργασία ΠΠΤ
3.	Υποχρεώσεις προς εντολείς ΠΠΤ 3.1. Υποχρεώσεις προς εντολείς ΠΠΤ
4.	Απόρρητο από το σχεδιασμό και απόρρητο εξ ορισμού 4.1. Προσωρινά αρχεία 4.2. Επιστροφή, μεταφορά ή απόρριψη ΠΠΤ 4.3. Έλεγχοι μετάδοσης ΠΠΤ
5.	Κοινή χρήση, μεταφορά και αποκάλυψη ΠΠΤ 5.1. Βάση για μεταφορά ΠΠΤ μεταξύ δικαιοδοσιών 5.2. Χώρες και διεθνείς οργανισμοί όπου μπορούν να μεταφερθούν ΠΠΤ 5.3. Αρχεία αποκάλυψης ΠΠΤ σε τρίτους 5.4. Ειδοποίηση αιτημάτων αποκάλυψης ΠΠΤ 5.5. Νομικώς δεσμευτικές γνωστοποιήσεις ΠΠΤ 5.6. Γνωστοποίηση υπεργολάβων που χρησιμοποιούνται για την επεξεργασία ΠΠΤ 5.7. Πρόσληψη υπεργολάβου για την επεξεργασία ΠΠΤ 5.8. Αλλαγή υπεργολάβου για επεξεργασία ΠΠΤ

Σχετικά με την επιθεώρηση που διενεργείται στα πλαίσια της επιτήρησης της πιστοποίησης ή της επαναπιστοποίησης ισχύουν τα όσα αναφέρονται στον Γενικό Κανονισμό Πιστοποίησης ΣΔ (**ΓΚΠΣΔ**).

4.4.Αξιολόγηση της Συμμόρφωσης του ΣΔΠΙ

Το ποσοστό συμμόρφωσης του επιθεωρούμενου ΣΔΠΙ με τις ελάχιστες απαιτήσεις του προτύπου ISO/IEC 27701, επιπρόσθετα με αυτές του προτύπου ISO/IEC 27001, εκτιμάται από τον Επικεφαλής Επιθεωρητή βασιζόμενη σε ευρήματα της επιθεώρησης. Τονίζεται δε ότι στην έκθεση επιθεώρησης συμπεριλαμβάνεται η επισκόπηση της επιθεώρησης της **αξιολόγησης αντικτύπου στο απόρρητο των πληροφοριών** (***Privacy Impact Assessment-PIA***) του πελάτη ή αναφορά σε αυτήν.

4.5.Χορήγηση Πιστοποίησης ΣΔΠΙ

Η απόφαση χορήγησης του αντίστοιχου πιστοποιητικού εγκρίνεται από τον Υπεύθυνο Πιστοποίησης ΣΔ του Φορέα έπειτα από την επιτυχή ανασκόπηση της συνταχθείσας από τον Επικεφαλής Επιθεωρητή έκθεσης αξιολόγησης της συμμόρφωσης του ΣΔΠΙ, εφόσον δεν υπάρχει μη συμμόρφωση που επιφέρει επιπτώσεις στη συμμόρφωση κατά ISO/IEC 27001. Τόσο η ανασκόπηση της έκθεσης όσο και η απόφαση χορήγησης της πιστοποίησης διεξάγεται από άτομο που πληροί τις απαιτήσεις επάρκειας όπως αυτές ορίζονται στο πρότυπο ISO/IEC TS 27006-2:2021 (παρ. 7.1.2.2). Η απόφαση οδηγεί στην χορήγηση του αντίστοιχου πιστοποιητικού ΣΔΠΙ τριετούς διάρκειας (στην περίπτωση αρχικής πιστοποίησης), της διατήρησης του υπάρχοντος (στην περίπτωση ετήσιας επιτήρησης) ή της επέκτασης της διάρκειας ισχύος του για ακόμα τρία (3) έτη (στην περίπτωση επαναπιστοποίησης).

Σημειώνεται ότι στην τεκμηρίωση της πιστοποίησης ΣΔΠΙ (π.χ. έκθεση επιθεώρησης, πιστοποιητικό):

- καθορίζεται ο ρόλος του πελάτη ως ελεγκτής ή/και επεξεργαστής ΠΠΤ για κάθε δραστηριότητα, προϊόν ή/και υπηρεσία εντός του πεδίου εφαρμογής της πιστοποίησης ΣΔΠΙ,
- διασφαλίζεται η ορθή οριοθέτηση του πεδίου εφαρμογής της πιστοποίησης ΣΔΠΙ εντός των δραστηριοτήτων του πελάτη που ορίζονται τόσο στο πεδίο εφαρμογής του ΣΔΠΙ και στη Δήλωση Εφαρμοσιμότητας (SoA) όσο και στο πεδίο εφαρμογής της πιστοποίησης ΣΔΑΠ,
- καθορίζεται η πιστοποίηση ΣΔΑΠ στην οποία θα βασιστεί η πιστοποίηση ΣΔΠΙ,
- καθορίζεται η συμμόρφωση του ΣΔΠΙ με το πρότυπο ISO/IEC 27701,
- συμπεριλαμβάνεται η Δήλωση Εφαρμοσιμότητας (SoA) κατά ISO/IEC 27001 και κατά ISO/IEC 27701, εφόσον τηρούνται χωριστά,

- η ημερομηνία λήξης της πιστοποίησης ΣΔΠΙ δεν θα υπερβαίνει την ημερομηνία λήξης της πιστοποίησης ΣΔΑΠ στο οποίο βασίζεται το ΣΔΠΙ.

Σχετικά με την πιστοποίηση πολλαπλών εγκαταστάσεων και τη μεταφορά πιστοποίησης από άλλον διαπιστευμένο Φορέα Πιστοποίησης ισχύουν τα όσα αναφέρονται στο Γενικό Κανονισμό Πιστοποίησης ΣΔ (**ΓΚΠΣΔ**).

Σημειώνεται ότι η απόφαση για την αναστολή, ανάκληση ή μείωση του πεδίου εφαρμογής της πιστοποίησης ΣΔΑΠ ενός πελάτη επιφέρει αυτόματα την ίδια απόφαση για την πιστοποίηση και του ΣΔΠΙ του πελάτη, εφόσον αυτή υφίσταται.

5. Ιστορικό Εκδόσεων

Ο παρών Ειδικός Κανονισμός Πιστοποίησης Συστημάτων Διαχείρισης του Φορέα ενδέχεται να υποστεί αλλαγές ή αναθεωρήσεις, μερικώς ή στο σύνολό του, ύστερα από την έγκριση της Επιτροπής Αμεροληψίας. Οι καινούργιες εκδόσεις του δημοσιοποιούνται έπειτα στην επίσημη ιστοσελίδα του Φορέα.

Αριθμός Αναθ. Έκδοσης	Περιγραφή Αναθεώρησης	Ισχύει από
1.0	Αρχική έκδοση	09-06-2023
1.1	Ενσωμάτωση του ISO/IEC TS 27006-2:2021	25-08-2023