Ειδικός Κανονισμός Πιστοποίησης Συστημάτων Διαχείρισης Πιστοποίηση Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) κατά ISO/IEC 27001:2022

1. Ειδικές Προδιαγραφές Πιστοποίησης ΣΔΑΠ

Η αρχική πιστοποίηση, όπως επίσης και οι επιτηρήσεις της πιστοποίησης και η επαναπιστοποίηση, **Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών** (**ΣΔΑΠ**) κατά **ISO/IEC 27001:2022** βασίζονται στις γενικές απαιτήσεις, όπως αυτές αναγράφονται στο Γενικό Κανονισμό Πιστοποίησης Συστημάτων Διαχείρισης (**ΓΚΠΣΔ**), και πιο συγκεκριμένα σε αυτές των ισχυουσών εκδόσεων των κάτωθι:

- **ISO/IEC 27001:2022** «Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία ιδιωτικότητας – Συστήματα διαχείρισης της ασφάλειας πληροφοριών – Απαιτήσεις»
- **ΕΛΟΤ ΕΝ ISO/IEC 27002:2022** «Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία ιδιωτικότητας - Έλεγχοι προστασίας 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»
- **IAF MD26:2023** «Απαιτήσεις μετάβασης στο ISO/IEC 27001:2022»

2. Περιγραφή της Πιστοποίησης ΣΔΑΠ

Η πιστοποίηση του ΣΔΑΠ ενός οργανισμού κατά ISO/IEC 27001:2022 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 της Ασφάλειας των Πληροφοριών. Η συμμόρφωση αυτή έγκειται σε απόδειξη:

- της δυνατότητας και ακρίβειας κατά την συντήρηση και τη διαρκείς βελτίωση ενός Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών,
- την εκτίμηση και την διαχείριση των κινδύνων ασφάλειας των πληροφοριών.

Τονίζεται ότι το πρότυπο ISO/IEC 27001:2022 υλοποιείται σε οποιονδήποτε οργανισμό, ανεξαρτήτως της έκτασης και του χρήσης του, όπως και των προϊόντων που προσφέρει.

Το ISO/IEC 27001 είναι το πλέον κατάλληλο διεθνές πρότυπο που αναγνωρίζεται παγκοσμίως για τη διαχείριση κινδύνων για την ασφάλεια των πληροφοριών που συντηρείται από μια εταιρία. Η πιστοποίηση κατά το πρότυπο ISO/IEC 27001 δίνει στον Οργανισμό την δυνατότητα να αποδείξει στους πελάτες του αλλά και σε άλλα ενδιαφερόμενα μέρη ότι διαχειρίζεται ορθά την ασφάλεια των πληροφοριών του. Η τελευταία έκδοσή του (2022) διαθέτει ένα σύνολο τυποποιημένων απαιτήσεων για ένα ολοκληρωμένο ΣΔΑΠ. Το πρότυπο ενστερνίζεται μια προσέγγιση βασισμένη στη διαδικασία για τη σύνθεση, την εκτέλεση, τη λειτουργία, την επιτήρηση, τη συντήρηση και τη βελτίωση του ΣΔΑΠ κάθε οργανισμού.

3. Τύπος Πιστοποιητικού

Το πιστοποιητικό που εκδίδεται από τον Φορέα Πιστοποίησης UCERT αναφέρεται στην πιστοποίηση **ΣΔΑΠ** κατά ISO/IEC 27001:2022.

4.Διαδικασία Πιστοποίησης ΣΔΑΠ

Ο Φορέας Πιστοποίησης UCERT αναλαμβάνει να εκτιμήσει την εναρμόνιση του **ΣΔΑΠ** ενός οργανισμού με τις προδιαγραφές του διεθνούς προτύπου **ISO/IEC 27001:2022**, 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 27006 και της διαδικασίας **Δ36**) και των μελών του Μητρώου Επιθεωρητών/Εμπειρογνωμόνων Πιστοποίησης ΣΔ.

4.1.Στάδια Επιθεώρησης ΣΔΑΠ

Η διαδικασία της επιθεώρησης αποτελείται από δύο στάδια, τα οποία διενεργούνται στις εγκαταστάσεις του πελάτη, ύστερα από την ενημέρωσή του για τα αντίστοιχα σχέδια επιθεώρησης. Ειδικότερα, στο 1ο στάδιο υπάρχει η δυνατότητα να μην γίνει στις εγκαταστάσεις του Πελάτη, εάν ικανοποιούνται συγκεκριμένες προϋποθέσεις: χωρίς πολλαπλές εγκαταστάσεις και με απλό πεδίο δραστηριοτήτων μικρής διακινδύνευσης.

4.2.Επιθεωρητές ΣΔΑΠ

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

Τα μέλη του Μητρώου είναι πεπειραμένοι επιθεωρητές ΣΔΑΠ κατά ISO/IEC 27001:2022 και η επάρκειά τους αναλύεται στη διαδικασία **Δ36-3**.

Ο Επικεφαλής Επιθεωρητής διεξάγει και τα δύο στάδια της επιθεώρησης, τόσο κατά την αρχική πιστοποίηση ενός ΣΔΑΠ, 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 ΣΔΑΠ 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 ΣΔΑΠ, αλλά και τη λειτουργία και τα αγαθά των υπό πιστοποίηση ΣΔΑΠ των οργανισμών
- Μη ύπαρξη σχέσης (οικονομικής, εμπορικής ή οποιουδήποτε άλλου είδους) με τον οργανισμό του οποίου το ΣΔΑΠ 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 ΣΔΑΠ

Μετά την έγκριση της αίτησης αρχικής πιστοποίησης του ΣΔΑΠ 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.

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 ΣΔΑΠ 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 ΣΔΑΠ 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 ΣΔΑΠ

Η επιθεώρηση που διενεργείται είναι διαρθρωμένη όμοια με το πρότυπο ISO/IEC 27001:2022. Επιγραμματικά στον παρακάτω πίνακα αναφέρονται οι απαιτήσεις του προτύπου με τις οποίες ο οργανισμός πρέπει να εναρμονίζεται:

§	Απαιτήσεις
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 της Ασφάλειας Πληροφοριών 4. Σύστημα Διαχείρισης της Ασφάλειας Πληροφοριών (και διεργασίες του)
5.	**Ηγεσία** 1. Ηγεσία και δέσμευση 2. Πολιτική 3. Ρόλοι, υπευθυνότητες και αρμοδιότητες εντός του οργανισμού
6.	**Σχεδιασμός** 1. Ενέργειες για την αντιμετώπιση απειλών και την αξιοποίηση ευκαιριών 1.1. Γενικά 1.2. Αξιολόγηση κινδύνων σχετικών με την ασφάλεια πληροφοριών 1.3. Αντιμετώπιση κινδύνων σχετικών με την ασφάλεια πληροφοριών 2. Στόχοι ασφάλειας πληροφοριών και σχεδιασμός για την επίτευξή τους 3. Σχεδιασμός αλλαγών
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
8.	**Λειτουργία** 1. Σχεδιασμός και έλεγχος της λειτουργίας (διεργασιών) 2. Αξιολόγηση κινδύνων σχετικών με την ασφάλεια πληροφοριών 3. Αντιμετώπιση κινδύνων σχετικών με την ασφάλεια πληροφοριών
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
10.	**Βελτίωση** 1. Συνεχής βελτίωση 2. Μη συμμόρφωση και διορθωτικές ενέργειες
Α.5.	**Οργανωτικοί έλεγχοι** 1. Πολιτικές ασφάλειας πληροφοριών 2. Ρόλοι και υπευθυνότητες ασφάλειας πληροφοριών 3. Διαχωρισμός καθηκόντων 4. Ευθύνες διαχείρισης 5. Επικοινωνία με τις αρχές

§	Απαιτήσεις
	6. Επικοινωνία με ειδικές ομάδες ενδιαφέροντος 7. Ευφυία απειλών 8. Ασφάλεια πληροφοριών στη διαχείριση έργων 9. Απογραφή πληροφοριών και άλλων συναφών περιουσιακών στοιχείων 10. Αποδεκτή χρήση πληροφοριών και άλλων συναφών περιουσιακών στοιχείων 11. Επιστροφή περιουσιακών στοιχείων 12. Διαβάθμιση πληροφοριών 13. Επισήμανση πληροφοριών 14. Μεταφορά (ανταλλαγή) πληροφοριών 15. Έλεγχος πρόσβασης 16. Διαχείριση ταυτότητας (χρήστη) 17. Πληροφορίες αυθεντικοποίησης 18. Δικαιώματα πρόσβασης (χρηστών) 19. Ασφάλεια πληροφοριών στις σχέσεις με προμηθευτές 20. Αντιμετώπιση της ασφάλειας πληροφοριών σε συμφωνίες με τρίτους/προμηθευτές 21. Διαχείριση της ασφάλειας πληροφοριών στην εφοδιαστική αλυσίδα των ΤΠΕ 22. Παρακολούθηση, ανασκόπηση και διαχείριση αλλαγών των υπηρεσιών προμηθευτών 23. Ασφάλεια Πληροφοριών για τη χρήση υπηρεσιών υπολογιστικού νέφους (cloud) 24. Σχεδιασμός και προετοιμασία διαχείρισης συμβάντων ασφάλειας πληροφοριών 25. Αξιολόγηση και λήψη απόφασης επί συμβάντων ασφάλειας πληροφοριών 26. Ανταπόκριση σε συμβάντα ασφάλειας πληροφοριών 27. Μάθηση από συμβάντα ασφάλειας πληροφοριών 28. Συλλογή αποδεικτικών στοιχείων 29. Ασφάλεια πληροφοριών κατά τη διάρκεια διακοπής 30. Ετοιμότητα των ΤΠΕ για επιχειρηματική συνέχεια 31. Νομικές, νομοθετικές, κανονιστικές και συμβατικές απαιτήσεις 32. Δικαιώματα πνευματικής ιδιοκτησίας 33. Προστασία εγγραφών/αρχείων/μητρώων 34. Ιδιωτικότητα και προστασία Πληροφοριών Προσωπικής Ταυτοποίησης-ΠΠΤ (*Personally Identifiable Information-PII*) 35. Ανεξάρτητος έλεγχος της ασφάλειας πληροφοριών 36. Συμμόρφωση με πολιτικές, κανόνες και προδιαγραφές για την ασφάλεια πληροφοριών 37. Τεκμηριωμένες διαδικασίες λειτουργίας
Α.6.	**<u>Έλεγχοι σε ανθρώπους</u>** 1. Διαλογή (Screening) 2. Όροι και συνθήκες απασχόλησης 3. Ευαισθητοποίηση, εκπαίδευση και κατάρτιση σχετικά με την ασφάλεια πληροφοριών 4. Πειθαρχική διαδικασία 5. Υπευθυνότητες μετά τη λήξη ή την αλλαγή της απασχόλησης 6. Συμφωνίες εμπιστευτικότητας ή μη-αποκάλυψης 7. Απομακρυσμένη εργασία (τηλε-εργασία) 8. Αναφορά συμβάντων ασφάλειας πληροφοριών
Α.7.	**<u>Φυσικοί έλεγχοι</u>** 1. Περίμετροι φυσικής ασφάλειας 2. Φυσική πρόσβαση 3. Προστασία γραφείων, δωματίων και (λοιπών) εγκαταστάσεων 4. Παρακολούθηση φυσικής ασφάλειας 5. Προστασία από φυσικές και περιβαλλοντικές απειλές 6. Εργασία σε ασφαλείς περιοχές 7. «Καθαρό γραφείο» και «καθαρή οθόνη» 8. Εγκατάσταση (τοποθέτηση) και προστασία εξοπλισμού 9. Ασφάλεια περιουσιακών στοιχείων εκτός εγκαταστάσεων 10. Μέσα αποθήκευσης 11. Υποστηρικτικά βοηθητικά εργαλεία/προγράμματα 12. Ασφάλεια καλωδιώσεων 13. Συντήρηση εξοπλισμού

§	Απαιτήσεις
	14. Ασφαλής καταστροφή (απόρριψη) ή επαναχρησιμοποίηση εξοπλισμού
Α.8.	**Τεχνολογικοί έλεγχοι** 1. Συσκευές τελικού σημείου χρήστη 2. Προνομιακά δικαιώματα πρόσβασης 3. Περιορισμός πρόσβασης σε πληροφορίες 4. Πρόσβαση σε πηγαίο κώδικα (εφαρμογών) 5. Ασφαλής αυθεντικοποίηση (έλεγχος ταυτότητας) 6. Διαχείριση χωρητικότητας πόρων 7. Προστασία από κακόβουλο λογισμικό 8. Διαχείριση τεχνικών ευπαθειών 9. Διαχείριση διαμορφώσεων ασφάλειας 10. Διαγραφή πληροφοριών 11. Απόκρυψη δεδομένων 12. Πρόληψη διαρροής δεδομένων 13. Αντίγραφα ασφάλειας πληροφοριών 14. Πλεονασμός εγκαταστάσεων επεξεργασίας πληροφοριών 15. Καταγραφή (ενεργειών χρηστών) 16. Δραστηριότητες παρακολούθησης 17. Συγχρονισμός ρολογιών 18. Προνομιακή χρήση βοηθητικών εργαλείων/προγραμμάτων (συστήματος) 19. Εγκατάσταση λογισμικού στα επιχειρησιακά συστήματα 20. Ασφάλεια δικτύων 21. Ασφάλεια δικτυακών υπηρεσιών 22. Διαχωρισμός δικτύων 23. Φιλτράρισμα Παγκόσμιου Ιστού 24. Χρήση κρυπτογραφίας 25. Ασφαλής κύκλος ζωής ανάπτυξης 26. Απαιτήσεις ασφάλειας εφαρμογών 27. Αρχές αρχιτεκτονικής και μηχανικής ασφαλούς συστήματος 28. Ασφαλής κωδικοποίηση (παραγωγή κώδικα λογισμικού) 29. Δοκιμές ασφάλειας κατά την ανάπτυξη και αποδοχή 30. Ανάπτυξη εφαρμογών από τρίτους (εξωτερική ανάθεση) 31. Διαχωρισμός περιβαλλόντων ανάπτυξης, δοκιμής και παραγωγής 32. Διαχείριση αλλαγών 33. Πληροφορίες δοκιμών 34. Προστασία πληροφοριακών συστημάτων κατά τη διάρκεια δοκιμών ελέγχου τους

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 ΣΔΑΠ

Το ποσοστό συμμόρφωσης του επιθεωρούμενου ΣΔΑΠ με τις ελάχιστες απαιτήσεις του προτύπου ISO/IEC 27001:2022 εκτιμάται από τον Επικεφαλής Επιθεωρητή βασιζόμενη σε ευρήματα της επιθεώρησης.

4.5.Χορήγηση Πιστοποίησης ΣΔΑΠ

Η απόφαση χορήγησης του αντίστοιχου πιστοποιητικού εγκρίνεται από τον Υπεύθυνο Πιστοποίησης ΣΔ του Φορέα έπειτα από την έκθεση αξιολόγησης της συμμόρφωσης του ΣΔΑΠ, συνταχθείσα από τον Επικεφαλής Επιθεωρητή και έγκριση του πρώτου. Η απόφαση οδηγεί στην χορήγηση του αντίστοιχου πιστοποιητικού ΣΔΑΠ 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).

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**).

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	30-05-2023