Ειδικός Κανονισμός Πιστοποίησης Συστημάτων Διαχείρισης Πιστοποίηση Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) κατά ΕΛΟΤ ISO/IEC 27001:2013

1. Ειδικές Προδιαγραφές Πιστοποίησης ΣΔΑΠ

Η αρχική πιστοποίηση, όπως επίσης και οι επιτηρήσεις της πιστοποίησης και η επαναπιστοποίηση, **Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών** (**ΣΔΑΠ**) κατά **ΕΛΟΤ ISO/IEC 27001:2013** βασίζονται στις γενικές απαιτήσεις, όπως αυτές αναγράφονται στο Γενικό Κανονισμό Πιστοποίησης Συστημάτων Διαχείρισης (**ΓΚΠΣΔ**), και πιο συγκεκριμένα σε αυτές των ισχυουσών εκδόσεων των κάτωθι:

- **ΕΛΟΤ EN ISO/IEC 17021-1** «Αξιολόγηση της συμμόρφωσης – Απαιτήσεις για φορείς επιθεώρησης και πιστοποίησης Συστημάτων Διαχείρισης – Μέρος 1: Απαιτήσεις»
- **ISO/IEC 27002/2013** «Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κώδικας πρακτικής για τους ελέγχους ασφάλειας των πληροφοριών»
- **ISO/IEC 27006** «Απαιτήσεις για Οργανισμούς που διενεργούν επιθεωρήσεις σε Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών»
- **ΕΛΟΤ ISO/IEC 27001** «Τεχνολογία πληροφοριών – Τεχνικές ασφάλειας – Συστήματα διαχείρισης της ασφάλειας πληροφοριών – Απαιτήσεις»
- **ΕΣΥΔ-ΚΑΔ** «Κανονισμός Διαπίστευσης του Εθνικού Συστήματος Διαπίστευσης»
- **IAF MD01** «Κατευθυντήρια Οδηγία για τη πιστοποίηση πολλαπλών εγκαταστάσεων με δειγματοληπτική επιλογή»
- **IAF MD02** «Κατευθυντήρια Οδηγία για μεταφορά της πιστοποίησης από ΦΠ σε ΦΠ»
- **IAF MD03** «Κατευθυντήρια Οδηγία για σύνθετη επιτήρηση και διαδικασίες επαναπιστοποίησης»
- **IAF MD04** «Κατευθυντήρια Οδηγία για τη χρήση υποβοήθησης μέσω Η/Υ τεχνικών επιθεώρησης για διαπιστευμένη πιστοποίηση Συστημάτων Διαχείρισης»
- **IAF MD05** «Κατευθυντήρια Οδηγία για το καθορισμό ανθρωποχρόνου επιθεώρησης Συστημάτων Διαχείρισης Ποιότητας και Περιβαλλοντικής Διαχείρισης»
- **IAF MD10** «Κατευθυντήρια Οδηγία για την αξιολόγηση της διαχείρισης Επάρκειας ενός Φορέα Πιστοποίησης σύμφωνα με το ISO/IEC 17021:2011»
- **IAF MD11** «Κατευθυντήρια οδηγία για την εκτέλεση συνδυαστικής επιθεώρησης ταυτόχρονα για περισσότερα του ενός ΣΔ»
- **IAF MD19** «Κατευθυντήρια οδηγία για τη πιστοποίηση πολλαπλών εγκαταστάσεων όταν δεν είναι κατάλληλη η δειγματοληπτική επιλογή εγκαταστάσεων»

2. Περιγραφή της Πιστοποίησης ΣΔΑΠ

Η πιστοποίηση του ΣΔΑΠ ενός οργανισμού κατά ΕΛΟΤ ISO/IEC 27001:2013 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 ΕΛΟΤ ISO/IEC 27001:2013 υλοποιείται σε οποιονδήποτε οργανισμό, ανεξαρτήτως της έκτασης και του χρήσης του, όπως και των προϊόντων που προσφέρει.

Το ISO 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 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 (2013) 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 ΕΛΟΤ ISO/IEC 27001:2013.

4. Διαδικασία Πιστοποίησης ΣΔΑΠ

Ο Φορέας Πιστοποίησης UCERT αναλαμβάνει να εκτιμήσει την εναρμόνιση του **ΣΔΑΠ** ενός οργανισμού με τις προδιαγραφές του διεθνούς προτύπου **ΕΛΟΤ ISO/IEC 27001:2013**, 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 27006:2015 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, έπειτα αποδοχής του αντίστοιχου σχεδίου επιθεώρησης από την πλευρά του. 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.

Αναλυτικά, τα μέλη του Μητρώου είναι πεπειραμένοι επιθεωρητές ΣΔΑΠ κατά ΕΛΟΤ ISO/IEC 27001:2013, των οποίων η εμπειρογνωμοσύνη αποδεικνύεται με έναν από τους παρακάτω τρόπους (διαδικασία **Δ36**):

- Βεβαίωση περάτωσης εγκεκριμένου προγράμματος εκπαίδευσης
- Πιστοποιητικό ως επιθεωρητής ΣΔΑΠ χορηγούμενο από διαπιστευμένο κατά ISO 17024 Φορέα ή με άλλο ισοδύναμο τρόπο
- Βεβαίωση επιμόρφωσης με αντικείμενο τη διενέργεια επιθεωρήσεων ΣΔΑΠ βάσει των ισχυόντων κανονιστικών και τυποποιητικών εγγράφων

Για την ενσωμάτωση μέλους του Μητρώου στην ομάδα επιθεώρησης ενός ΣΔΑΠ λαμβάνονται υπόψη τα κάτωθι:

- Πληρότητα των απαιτήσεων επάρκειάς του όπως αυτές ορίζονται στο ISO/IEC 27006:2015
- Τίτλοι σπουδών
- Εμπειρία σε επιθεωρήσεις κατά την τελευταία τριετία:
  - μία (1) μέχρι τρεις (3) επιθεωρήσεις για τη συμμόρφωση ΣΔΑΠ στην ισχύουσα έκδοση του προτύπου ΕΛΟΤ ISO/IEC 27001, ή στην προηγούμενη εφόσον υπήρξε κατάλληλη επιμόρφωση για τη μετάβαση στην ισχύουσα, και σε πεδίο συναφές με τα προσόντα του και

- επιτυχή επιτόπια αξιολόγησή του σε επιθεώρηση με βαθμό διακινδύνευσης τουλάχιστον μέτριο

➢ Διενέργεια επιθεωρήσεων εκ μέρους άλλων διαπιστευμένων Φορέων Πιστοποίησης ή του Ε.ΣΥ.Δ.

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 ΣΔΠ 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.

Στο ενδεχόμενο περισσότερων της μίας εγκαταστάσεων, ο Φορέας δύναται να επιλέξει ποιες απ' αυτές θα επιθεωρηθούν, εκτός αυτής που θεωρείται κεντρική (από όπου ασκείται η διοίκηση). Η πιστοποίηση του ΣΔΑΠ ενός σύνθετου οργανισμού αφορά τη εφαρμογή στο σύνολο του οργανισμού, με αποτέλεσμα να απαγορεύεται ο αποκλεισμός εγκατάστασης από την πιστοποίηση.

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 ΕΛΟΤ ISO/IEC 27001:2013. 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

§	Απαιτήσεις
	3. Ρόλοι, υπευθυνότητες και αρμοδιότητες εντός του οργανισμού
6.	**Σχεδιασμός**
	1. Ενέργειες για την αντιμετώπιση απειλών και την αξιοποίηση ευκαιριών
	2. Στόχοι ασφάλειας πληροφοριών και σχεδιασμός για την επίτευξή τους
7.	**Υποστήριξη**
	1. Πόροι
	2. Επαγγελματική επάρκεια
	3. Ευαισθητοποίηση
	4. Επικοινωνία
	5. Τεκμηριωμένες πληροφορίες
8.	**Λειτουργία**
	1. Σχεδιασμός, λειτουργία και έλεγχος των 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
	3. Ανασκόπηση από τη Διοίκηση
10.	**Βελτίωση**
	1. Μη συμμόρφωση και διορθωτικές ενέργειες
	2. Συνεχής βελτίωση
Α.5.	**Πολιτικές Ασφάλειας Πληροφοριών**
	1. Διαχείριση κατευθύνσεων για την ασφάλεια πληροφοριών
	1.1. Πολιτικές ασφάλειας πληροφοριών
	1.2. Ανασκόπηση πολιτικών ασφαλείας
Α.6.	**Οργάνωση Ασφάλειας Πληροφοριών**
	1. Εσωτερική οργάνωση
	1.1. Ρόλοι και αρμοδιότητες ασφάλειας πληροφοριών
	1.2. Καθορισμός καθηκόντων
	1.3. Επαφή με τις αρχές
	1.4. Επαφή με ειδικές ομάδες ενδιαφέροντος
	1.5. Ασφάλεια πληροφοριών στη διαχείριση έργου
	2. Τηλε-εργασία και απομακρυσμένη πρόσβαση
	2.1. Πολιτική κινητών συσκευών
	2.2. Τηλε-εργασία
Α.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 πληροφοριών
	2.3. Πειθαρχικές διαδικασίες
	3. Απόλυση/Αποχώρηση προσωπικού
	3.1. Αρμοδιότητες λήξης ή αλλαγής εργασίας
Α.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

§	Απαιτήσεις
	3. Διαχείριση μέσων αποθήκευσης 3.1. Διαχείριση φορητών μέσων αποθήκευσης 3.2. Καταστροφή μέσων αποθήκευσης 3.3. Διακινούμενα φυσικά μέσα
Α.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. Πρόβλεψη 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. Ασφαλής διαδικασία εισόδου 4.3. Διαχείριση συνθηματικών συστήματος 4.4. Χρήση εργαλείων συστήματος 4.5. Έλεγχος πρόσβασης στον πηγαίο κώδικα των εφαρμογών
Α.10.	**Κρυπτογραφία** 1. Κρυπτογραφικά εργαλεία 1.1. Πολιτική χρήσης κρυπτογραφικών εργαλείων 1.2. Διαχείριση κλειδιών
Α.11.	**Φυσική Ασφάλεια Χώρων** 1. Ασφαλείς περιοχές 1.1. Περίμετρος φυσικής ασφαλείας 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 αγαθών 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
Α.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 ασφαλείας πληροφοριών

§	Απαιτήσεις
	4. Καταγραφή και παρακολούθηση 4.1. Καταγραφή ενεργειών χρηστών 4.2. Προστασία αρχείων καταγραφής 4.3. Αρχεία καταγραφής Διαχειριστών 4.4. Συγχρονισμός ρολογιών 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
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
Α.14.	**Προμήθεια, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων** 1. Απαιτήσεις ασφάλειας πληροφοριακών συστημάτων 1.1. Ανάλυση και προσδιορισμός απαιτήσεων ασφαλείας 1.2. Προστασία υπηρεσιών εφαρμογών σε δημόσια δίκτυα 1.3. Προστασία συναλλαγών 2. Ασφάλεια 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 ασφαλούς συστήματος Μηχανικής 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
Α.15.	**Σχέσεις με Προμηθευτές** 1. Ασφάλεια πληροφοριών στις σχέσεις με προμηθευτές 1.1. Πολιτική Ασφάλειας Πληροφοριών για τη σχέση με τους προμηθευτές 1.2. Αντιμετώπιση ασφαλείας σε συμφωνίες με τρίτους 1.3. Τεχνολογία επικοινωνιών και πληροφοριών εφοδιαστικής αλυσίδας 2. Διαχείριση παροχής υπηρεσιών από προμηθευτές 2.1. Παρακολούθηση και ανασκόπηση υπηρεσιών από προμηθευτές 2.2. Διαχείριση αλλαγών σε υπηρεσίες τρίτων
Α.16.	**Διαχείριση Περιστατικών Ασφάλειας Πληροφοριών** 1. Διαχείριση περιστατικών ασφάλειας και βελτιώσεις 1.1. Αρμοδιότητες και διαδικασίες 1.2. Αναφορά περιστατικών ασφαλείας 1.3. Αναφορά αδυναμιών ασφαλείας 1.4. Αξιολόγηση και εκτίμηση συμβάντων ασφαλείας 1.5. Ανταπόκριση περιστατικών ασφαλείας 1.6. Μάθηση από περιστατικά ασφαλείας

§	Απαιτήσεις
	1.7. Συλλογή πειστηρίων
Α.17.	**Διαχείριση Επιχειρησιακής Συνέχειας**
	1. Ασφάλεια πληροφοριών για την επιχειρησιακή συνέχεια 1.1. Σχεδιασμός επιχειρησιακής συνέχειας για την ασφάλεια πληροφοριών 1.2. Ανάπτυξη επιχειρησιακής συνέχειας για την ασφάλεια πληροφοριών 1.3. Επαλήθευση, ανασκόπηση και αξιολόγηση ασφάλειας πληροφοριών για την επιχειρησιακή συνέχεια 2. Επάρκεια πληροφοριών 2.1. Διαθεσιμότητα των εγκαταστάσεων επεξεργασίας της πληροφορίας
Α.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 πληροφοριών 2.1. Ανεξάρτητος έλεγχος της ασφάλειας 2.2. Συμμόρφωση με πολιτικές και προδιαγραφές ασφαλείας 2.3. Ανασκόπηση τεχνικής συμμόρφωσης

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 ΕΛΟΤ ISO/IEC 27001:2013 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	04-07-2020