Κανονισμός Πιστοποίησης Συστημάτων Ασφάλειας Πληροφοριών

Πρότυπο ή Σχήμα πιστοποίησης:	**ISO 27001:2013 - ISO/IEC 27001:2022** **ISO 27701:2019**	**Πρότυπο Διαπίστευσης:**	**ISO 17021-1:2015**

Κύκλος Πιστοποίησης:

Το πιστοποιητικό έχει τριετή διάρκεια. Για τη διατήρηση της ισχύος του πιστοποιητικού διεξάγονται ετήσιες επιθεωρήσεις επιτήρησης. Πριν τη λήξη της ισχύος του πιστοποιητικού διεξάγεται επιθεώρηση επαναπιστοποίησης στην επιχείρηση για ανανέωση του πιστοποιητικού για την επόμενη τριετία.

Η επιθεώρηση Πιστοποίησης πραγματοποιείται σε δύο στάδια. Το Στάδιο 1 μπορεί να μην υλοποιηθεί στις εγκαταστάσεις του πελάτη. Το διάστημα μεταξύ των δύο σταδίων δεν μπορεί να υπερβαίνει τους έξι μήνες. Στην περίπτωση που παρέλθει αυτό το διάστημα ή προκύψουν σημαντικές αλλαγές που επηρεάζουν το Σύστημα Διαχείρισης, το Στάδιο 1 πρέπει να επαναληφθεί. Τα αποτελέσματα του Σταδίου 1 μπορούν να οδηγήσουν σε αναβολή ή ακύρωση του Σταδίου 2.

Προγραμματισμός επιθεωρήσεων και χρονοδιάγραμμα: οι επιθεωρήσεις επιτήρησης πρέπει να διεξάγονται ετησίως, με τελευταία ημερομηνία την ημέρα απόφασης Πιστοποίησης μετά την επιθεώρηση Αρχικής Πιστοποίησης. Αντίστοιχα, η επιθεώρηση Επαναπιστοποίησης πρέπει να ολοκληρώνεται μέσα στο ίδιο χρονικό περιθώριο. Για παράδειγμα:

Απόφαση Πιστοποίησης	**1η ετήσια επιτήρηση**	**2η ετήσια επιτήρηση**	**Επιθεώρηση Επαναπιστοποίησης**
15/7/2024	*15/7/2025*	*15/7/2026*	*15/7/2027*

Στην περίπτωση υπέρβασης των παραπάνω χρονικών ορίων, το πιστοποιητικό θα μπαίνει σε Παύση για έξι μήνες και μετά την παρέλευση του διαστήματος αυτού σε Ανάκληση.

Η ισχύουσα έκδοση της Δήλωσης Εφαρμογής (Statement of Applicability) αναγράφεται πάνω στο Πιστοποιητικό και ανασκοπείται κατά την επιθεώρηση. Ο πελάτης κατά τη διάρκεια λειτουργίας του συστήματος και διατήρησης του πιστοποιητικού οφείλει να ενημερώσει την TÜV AUSTRIA για οποιαδήποτε αλλαγή στη Δήλωση Εφαρμογής. Σε κάθε περίπτωση αλλαγή στην Δήλωση Εφαρμογής οδηγεί στην ακύρωση του προηγούμενου πιστοποιητικού και έκδοση νέου αφού εξετασθεί αν απαιτείται διεξαγωγή επιθεώρησης για την ανασκόπηση των αλλαγών. Ο γενικός κανόνας που ισχύει σε αυτές τις περιπτώσεις είναι ότι έκτακτη επιθεώρηση απαιτείται στην περίπτωση που νέα σημεία ελέγχου του προτύπου (Annex A) συμπεριληφθούν στο Σύστημα Διαχείρισης του πελάτη όπως αυτό θα φαίνεται μέσα από την Δήλωση Εφαρμογής.

Κατά την επιθεώρηση επαναπιστοποίησης μπορεί να απαιτηθεί η διεξαγωγή Σταδίου 1 αν έχουν υπάρξει σημαντικές αλλαγές στο Σύστημα Διαχείρισης ή στο πλαίσιο εντός του οποίου λειτουργεί (π.χ. αλλαγές στη νομοθεσία) και τον πελάτη.

Διεξαγωγή Επιθεωρήσεων ISO/IEC 27701

Για την απόκτηση πιστοποίησης κατά ISO/IEC27701, η πιστοποίηση κατά ISO/IEC 27001 είναι υποχρεωτική.

Το πεδίο εφαρμογής της πιστοποίησης ISO/IEC 27701

- ✔ είναι εντός ή ταυτόσημο του πεδίου εφαρμογής της πιστοποίησης ISO/IEC 27001.
- ✔ περιλαμβάνεται εντός των ορίων των δραστηριοτήτων του πελάτη όπως ορίζεται στο πεδίο εφαρμογής του PIMS.
- ✔ περιλαμβει την επεξεργασία PII

Η TÜV Austria θα παύει, θα ανακαλεί ή θα μειώνει το πεδίο εφαρμογής της πιστοποίησης του ISO/IEC 27701 όταν ανακαλείται, παύει ή μειώνεται το πεδίο εφαρμογής της βασικής της πιστοποίησης ISO/IEC 27001 (η οποία περιλαμβάνει το πεδίο εφαρμογής της

	πιστοποίησης ISO/IEC 27701).
Επιθεωρήσεις μετάβασης	Η TÜV Austria (TA) μπορεί να διεξάγει την επιθεώρηση μετάβασης σε συνδυασμό με την επιθεώρηση επιτήρησης, την επιθεώρηση επαναπιστοποίησης ή μέσω ξεχωριστής επιθεώρησης. Η επιθεώρηση μετάβασης δεν θα βασίζεται μόνο στην αναθεώρηση των εγγράφων, ιδίως για την αναθεώρηση των τεχνολογικών ελέγχων ασφάλειας πληροφοριών. Η επιθεώρηση μετάβασης περιλαμβάνει, αλλά δεν περιορίζεται στα ακόλουθα: ✔ Ανάλυση κενών (gap analysis) του ISO/IEC 27001:2022, καθώς και την ανάγκη για αλλαγές στα Συστήματα Διαχείρισης Πληροφορικής (ISMS) του πελάτη. ✔ Την ενημέρωση της δήλωσης εφαρμογής (ΔΕ). ✔ Εάν εφαρμόζεται, την ανανέωση του σχεδίου αντιμετώπισης κινδύνων. ✔ Την αποτελεσματικότητα των νέων ή τροποποιημένων μέτρων ελέγχου ασφάλειας πληροφοριών που έχουν επιλεχθεί από τους πελάτες. Η ΤΑ δύναται να διενεργεί την επιθεώρηση μετάβασης εξ αποστάσεως, εάν διασφαλίζει ότι επιτυγχάνονται οι στόχοι της επιθεώρησης μετάβασης. Μετά τη θετική απόφαση πιστοποίησης, το πιστοποιητικό εκδίδεται με βάση τον κύκλο πιστοποίησης του υφιστάμενου πιστοποιητικού ISO/IEC 27001:2013.
Χρονοδιάγραμμα μετάβασης	✔ Προβλέπεται μεταβατική περίοδος τριών ετών για την προσαρμογή στις απαιτήσεις του ISO/IEC 27001:2022, από την ημερομηνία έκδοσής του, έως τις 31.10.2025. ✔ Η μεταβατική περίοδος του ISO/IEC 27001:2022 λήγει στις 31.10.2025. Όλα τα πιστοποιητικά σύμφωνα με το ISO/IEC 27001:2013 θα ανακληθούν ή θα αποσυρθούν στο τέλος της μεταβατικής περιόδου. ✔ ΤΗ TÜV Austria θα δύναται να διεξάγει αρχικές επιθεωρήσεις ή επιθεωρήσεις επαναπιστοποίησης σύμφωνα με το ISO/IEC 27001:2013 έως τις 30.04.2024. Όλα τα πιστοποιητικά που εκδίδονται σύμφωνα με το ISO/IEC 27001:2013 κατά τη μεταβατική περίοδο πρέπει να λαμβάνουν υπόψη την παραπάνω προθεσμία (ανεξάρτητα από το αν θα συμπληρωθεί ή όχι η συνήθης τριετής περίοδος ισχύος του πιστοποιητικού). Οι οργανισμοί που διαθέτουν πιστοποιητικό ISO/IEC 27001:2013 θα έχουν τη δυνατότητα να μεταβούν στο νέο πρότυπο ISO/IEC 27001:2022 κατά τη διάρκεια των ετήσιων επιθεωρήσεων επιτήρησης ή επαναπιστοποίησης ή χωριστής επιθεώρησης μετάβασης, με προηγούμενη γραπτή ειδοποίηση της TÜV Austria.
Αξιολόγηση Κριτηρίων επιθεώρησης / Κατηγοριοποίηση Μη Συμμορφώσεων	**1:** Πλήρης συμμόρφωση **2:** Ευκαιρία Βελτίωσης: Δεν απαιτούνται ενέργειες από τον πελάτη **3**: Απλή Μη Συμμόρφωση(-εις) (Minor): Ανασκόπηση και αποδοχή του σχεδίου του πελάτη για διορθώσεις και διορθωτικές ενέργειες. Η αποτελεσματικότητα ανασκοπείται στην επόμενη επιθεώρηση **4:** Κύρια Μη Συμμόρφωση(-εις) (Major): Διόρθωση με προσκόμιση εγγράφων **5:** Κύρια Μη Συμμόρφωση(-εις) (Major): Διόρθωση με Επαναληπτική επιθεώρηση
Χρόνος αποκατάστασης Μη Συμμορφώσεων:	**Επιθεώρηση πιστοποίησης:** 2 μήνες μετά την ολοκλήρωση του σταδίου 2. **Επιθεώρηση επιτήρησης:** 2 μήνες μετά την ημερομηνία της επιθεώρησης ή το αργότερο μέχρι την ημερομηνία «επέτειο» της Απόφασης Πιστοποίησης. **Επιθεώρηση Επαναπιστοποίησης:** 2 μήνες μετά την ημερομηνία της επιθεώρησης ή το αργότερο μέχρι την ημερομηνία «επέτειο» της Απόφασης Πιστοποίησης.
Διάρκεια Σύμβασης	Η διάρκεια της υπηρεσίας και η συμβατική υποχρέωση τίθεται σε ισχύ με την υπογραφή και από τα δύο μέρη (TÜV AUSTRIA και Οργανισμό-Πελάτη) και ισχύει για (3) τρία έτη της

	σχετικής προσφοράς σε περιπτώσεις αρχικής πιστοποίησης ή επαναπιστοποίησης. Σε περίπτωση Διαπιστευμένης Μεταβίβασης Πιστοποίησης, η διάρκεια καλύπτει την περίοδο ισχύος του μεταβιβαζόμενου πιστοποιητικού. Σε περίπτωση μετάβασης σε νέα έκδοση του προτύπου, η διάρκεια της συμβατικής υποχρέωσης ισχύει μέχρι την ημερομηνία λήξης της πιστοποίησης που αναφέρεται στη σχετική παράγραφο του Κανονισμού.