|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ΕΠΩΝΥΜΙΑ ΕΠΙΧΕΙΡΗΣΗΣ:** | |  | | | |
| **ΔΙΕΘΥΝΣΗ:** | |  | | | |
| **ΕΚΠΡΟΣΩΠΟΣ ΕΠΙΧΕΡΗΣΗΣ:** | |  | | | |
| **ΠΡΟΤΥΠΟ:** | |  | | | |
| **ΕΙΔΟΣ ΕΠΙΘΕΩΡΗΣΗΣ:** | | **Συνδυαστική:**   **Ολοκληρωμένη:**  **Πολλαπλών Εγκαταστάσεων :**  **Μεταφορά:**   **Κοινό :** | | | |
| **ΤΥΠΟΣ ΕΠΙΘΕΩΡΗΣΗΣ:** | | **Αρχική:**  **Επιτήρηση:**  **Επαναπιστοποίηση:**  **Έκτακτη:** | | | |
| **ΤΟΠΟΣ ΔΙΕΞΑΓΩΓΗΣ/**  **ΧΡΟΝΟΣ:** | |  | | | |
| **ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΕΠΙΘΕΩΡΗΣΗΣ / ΔΙΑΡΚΕΙΑ:** | |  | | | |
| **ΗΜΕΡΟΜΗΝΙΑ (ΕΣ):** | |  | | | |
| **ΑΠΟΚΛΙΣΗ ΑΠΟ ΤΟΝ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟ:** | |  | | | |
| **ΚΩΔΙΚΟΣ ΕΡΓΟΥ:** | |  | | | |
| **ΟΜΑΔΑ ΕΠΙΘΕΩΡΗΣΗΣ** | | | | | |
| **ΕΠΙΚΕΦΑΛΗΣ ΕΠΙΕΘΩΡΗΤΗΣ** | | **ΕΠΙΘΕΩΡΗΤΗΣ** | **ΕΠΙΘΕΩΡΗΤΗΣ** | | **ΆΛΛΟ: ………………** |
|  | |  |  | |  |
| **ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ** | | | | | |
|  | | | | | |
| **ΔΗΛΩΣΗ ΕΦΑΡΜΟΓΗΣ (SOA)** | | | | | |
| **ΈΚΔΟΣΗ** | | **ΗΜ/ΝΙΑ ΕΚΔΟΣΗΣ** | **ΕΞΑΙΡΕΣΕΙΣ** | | |
|  | |  |  | | |
| **ΚΡΙΤΗΡΙΑ ΕΠΙΘΕΩΡΗΣΗΣ** | | | | | |
| Για την διεξαγωγή του 2ου σταδίου της επιθεώρησης/Επιτήρησης ανασκοπήθηκαν έγγραφα, δεδομένα, λειτουργίες και γνώσεις του προσωπικού ως προς τις αντίστοιχες απαιτήσεις του προτύπου ISO 27001:2013: | | | | | |
| Ελέγχθηκε | Απαίτηση Τεκμηρίωσης | | | | § ISO 27001:2013 |
|  | Πλαίσιο Λειτουργίας | | | | 4 |
|  | Πεδίο Εφαρμογής | | | | 4.3 |
|  | Πολιτική Ασφάλειας | | | | 5.3 |
|  | Διαδικασία αξιολόγησης κινδύνου | | | | 6.1 |
|  | Αποτελέσματα εφαρμογής της διαδικασίας αξιολόγησης κινδύνου | | | | 6.1  8.2 |
|  | Αντιμετώπιση Κινδύνου | | | | 6.1  8.3 |
|  | Δήλωση Εφαρμογής | | | | 6.1 |
|  | Στόχοι Ασφάλειας | | | | 6.2 |
|  | Διαχείριση Τεκμηριωμένης Πληροφορίας | | | | 7.5 |
|  | Διαδικασία διαχείρισης αλλαγών | | | | 8.1 |
|  | Παρακολούθηση, Μέτρηση και Ανάλυση | | | | 9.1 |
|  | Πρόγραμμα εσωτερικών επιθεωρήσεων | | | | 9.2 |
|  | Αποτελέσματα της τελευταίας εσωτερικής επιθεώρησης | | | | 9.2 |
|  | Πρακτικά της τελευταίας ανασκόπησης από τη διοίκηση | | | | 9.3 |
|  | Διαδικασία Διορθωτικών Ενεργειών | | | | 10.1 |
|  | Σχετικές Νομοθετικές και Κανονιστικές απαιτήσεις | | | | 4.2 |
|  | Συμβατικές υποχρεώσεις του οργανισμού (αν υπάρχουν) | | | | 4.2 |
|  | Διεργασίες που διενεργούνται από τρίτα μέρη | | | | 8.1 |
|  | Ρόλοι, αρμοδιότητες, Υπευθυνότητες, επαγγελματική επάρκεια, εκπαίδευση επικοινωνία και ενημέρωση | | | | 5.2, 7.2,  7.3, 7.4 |
|  | Μηχανισμοί ασφαλείας | | | | Παράρτημα Α. |
| **ΣΤΟΧΟΙ ΕΠΙΘΕΩΡΗΣΗΣ** | | | | | |
| Κατά τη διάρκεια του 2ου σταδίου της επιθεώρησης / επιτήρησης επιτεύχθηκαν οι ακόλουθοι στόχοι: | | | | | |
|  | Ανασκοπήθηκε η τεκμηριωμένη πληροφορία του επιθεωρούμενου συστήματος διαχείρισης. | | | | |
|  | Αξιολογήθηκε η εφαρμογή των πολιτικών, οδηγιών και διαδικασιών του οργανισμού. | | | | |
|  | Αξιολογήθηκαν οι συνθήκες που επικρατούν στον επιθεωρούμενο οργανισμό και διενεργήθηκαν συζητήσεις με το σχετικό προσωπικό. | | | | |
|  | Ανασκοπήθηκε η κατάσταση του επιθεωρούμενου οργανισμού και της κατανόησής του σχετικά με τις απαιτήσεις του προτύπου, ειδικά όσο αφορά την αναγνώριση των βασικών συστατικών στοιχείων, διεργασιών, στόχων κ.α. | | | | |
|  | Αξιολογήθηκε η αποτελεσματικότητα των εσωτερικών επιθεωρήσεων και της ανασκόπησης από τη διοίκηση. | | | | |
|  | Αξιολογήθηκε η ευθύνη της διοίκησης για τις πολιτικές | | | | |
|  | Αξιολογήθηκε η ικανότητα του συστήματος διαχείρισης να ικανοποιεί τις απαιτήσεις που προκύπτουν από νόμους, κανονισμούς και τις συμβάσεις με τρίτα μέρη. | | | | |
|  | Αξιολογήθηκε αν έχουν προκύψει σημαντικές αλλαγές στο σύστημα διαχείρισης. | | | | |
|  | Ελέγχθηκε η αποτελεσματικότητα των διορθωτικών ενεργειών επί των μη συμμορφώσεων της προηγούμενης επιθεώρησης. | | | | |
|  | Ελέγχθηκε η διαχείριση του σήματος πιστοποίησης. | | | | |
| **ΣΥΜΠΕΡΑΣΜΑΤΑ 2ΟΥ ΣΤΑΔΙΟΥ/ΕΠΙΤΗΡΗΣΗΣ** | | | | | |
| Βάση των παραπάνω, η ομάδα επιθεώρησης κατέληξε στα ακόλουθα συμπεράσματα: | | | | | |
| Το υπο εξέταση σύστημα διαχείρισης ασφάλειας πληροφοριών καλύπτει τις απαιτήσεις του προτύπου ISO 27001:2013 και κρίνεται αποτελεσματικό ως προς την κάλυψη των αναγνωρισμένων εφαρμόσιμων απαιτήσεων και των αναμενόμενων αποτελεσμάτων.  Το πεδίο εφαρμογής είναι κατάλληλο και οι στόχοι της επιθεώρησης έχουν καλυφθεί όπως φαίνεται παραπάνω. Οι υποχρεώσεις της επιχείρησης όσο αφορά το πιστοποιητικό, το σύστημα και το σήμα πιστοποίησης αναφέρονται στην σχετική σύμβαση.  Η επιθεώρηση είναι δειγματοληπτικού χαρακτήρα και ως εκ τούτου η μη καταγραφή αρνητικών ευρημάτων ενέχει βαθμό αβεβαιότητας χωρίς να σημαίνει ότι δεν υφίστανται αποκλίσεις στο εφαρμοζόμενο σύστημα διαχείρισης.  Η επιχείρηση οφείλει να τηρεί, συντηρεί και βελτιώνει το σύστημά της σύμφωνα με τις απαιτήσεις του σχετικού προτύπου (ISO 27001:2013).  Η παρούσα έκθεση δεν αποτελεί έκθεση ή απόδειξη για την νομική, κανονιστική ή συμβατική συμμόρφωση της επιχείρησης.  Η επιθεώρηση διενεργήθηκε βάσει της Διαδικασίας P 05 «Διαδικασία Επιθεωρήσεων», της EQA Hellas.  Για τη περίπτωση των μη συμμορφώσεων που εντοπίζονται κατά τη διάρκεια της αρχικής επιθεώρησης ή της επαναπιστοποίησης δίνεται ένα χρονικό διάστημα τριών μηνών για την αποκατάσταση τους, ενώ στις περιπτώσεις επιτήρησης το χρονικό διάστημα περιορίζεται στους δύο μήνες. Η αποτελεσματικότητα των ενεργειών που αφορά τις παρατηρήσεις κρίνεται στην επόμενη χρονικά επιθεώρηση.  Ο υπό επιθεώρηση Οργανισμός βρίσκεται σε λειτουργία και ελέγχεται το αιτούμενο πεδίο εφαρμογής της πιστοποίησης. Τα μέλη της ομάδας επιθεώρησης δεν έχουν καμμιά επαγγελματική ή άλλου είδους σχέση με τον επιθεωρούμενο οργανισμό τουλάχιστον για τα τελευταία δυο έτη. | | | | | |
|  | Η ομάδα επιθεώρησης εισηγείται ΘΕΤΙΚΑ για την έκδοση / διατήρηση πιστοποιητικού. | | | | |
|  | Η ομάδα επιθεώρησης εισηγείται ΘΕΤΙΚΑ για την έκδοση / διατήρηση πιστοποιητικού με την προϋπόθεση ότι οι Μη Συμμορφώσεις που αναφέρονται παραπάνω (ΕΥΡΗΜΑΤΑ 2ου ΣΤΑΔΙΟΥ/ΕΠΙΤΗΡΗΣΗΣ) θα αντιμετωπιστούν με επιτυχία και οι σχετικές αποδείξεις θα ελεγχθούν από τον Φορέα Πιστοποίησης σε διάστημα 3 μηνών για αρχική επιθεώρηση ή επαναπιστοποίηση και 2 μηνών για περιπτώσεις επιτήρησης. | | | | |
|  | Η ομάδα επιθεώρησης εισηγείται ΑΡΝΗΤΙΚΑ για την έκδοση πιστοποιητικού / Η ομάδα επιθεώρησης εισηγείται την ΑΝΑΚΛΗΣΗ του πιστοποιητικού | | | | |
|  | | | | | |
| **Συνεντεύξεις με το προσωπικό** | | | |  | |
| **Προσδιορισμός των οργανωτικών ή λειτουργικών μονάδων ή διεργασιών που επιθεωρήθηκαν και ο χρόνος της επιθεώρησης** | | | |  | |
| **Επιτόπιοι έλεγχοι στη περίπτωση ύπαρξης πολλαπλών εγκαταστάσεων (ημερομηνία, τοποθεσία, κλπ.)** | | | |  | |
| **Χρήση Λογοτύπων και Σημάτων σε έντυπη και ηλεκτρονική μορφή** | | | |  | |
| **Επαλήθευση της αποτελεσματικότητας των διορθωτικών ενεργειών που έχουν ληφθεί σε προηγούμενες εντοπισθείσες μη συμμορφώσεις- παρατηρήσεις** | | | |  | |
| **Ενδεχόμενες αποκλίσεις από το σχέδιο επιθεώρησης και αιτίες** | | | |  | |
| **Καταγραφή σημαντικών θεμάτων που επηρεάζουν το πρόγραμμα επιθεώρησης** | | | |  | |
| **Σημαντικές αλλαγές, εάν υπάρχουν, που επηρεάζουν το σύστημα διαχείρισης του πελάτη από την τελευταία επιθεώρηση που πραγματοποιήθηκε** | | | |  | |
| **Ερωτήματα / σχόλια / διαφωνίες/ Εκκρεμότητες** | | | |  | |
| **Συμπέρασμα σχετικά με την καταλληλότητα του πεδίου πιστοποίησης** | | | |  | |
| **Επιβεβαίωση ότι έχουν εκπληρωθεί οι αντικειμενικοί σκοποί της επιθεώρησης** | | | |  | |
| **Συμπερασματικά σχόλια περί συνολικής εφαρμογής και αποτελεσματικότητας επιθεωρούμενου ΣΔ** | | | |  | |
|  | | | | | |
| Ημερομηνία Σύνταξης της Αναφοράς: | | | | | |

|  |  |
| --- | --- |
| **ΣΥΜΜΕΤΕΧΟΝΤΕΣ EQA HELLAS (Ομάδα Επιθεώρησης):** | **ΣΥΜΜΕΤΕΧΟΝΤΕΣ ΠΕΛΑΤΗ ΚΑΤΑ ΤΗΝ ΚΑΤΑΛΗΚΤΙΚΗ ΣΥΝΕΔΡΙΑΣΗ:** |
| **17021-1:2015 § 9.4.7 Διεξαγωγή της καταληκτικής συνεδρίασης με την αναγκαία πληρότητα** | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ΑΠΟΚΛΙΣΕΙΣ** | | | | |
| **ΣΥΝΟΛΑ** | | | | |
| **ΜΗ ΣΥΜΜΟΡΦΩΣΕΙΣ:** | | **ΠΑΡΑΤΗΡΗΣΕΙΣ :** | **ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΒΕΛΤΙΩΣΗ:** | |
| **Α/Α ΜΗ ΣΥΜΜΟΡΦΩΣΗΣ:** | | **Α/Α ΠΑΡΑΤΗΡΗΣΗΣ:** | **Α/Α ΠΡΟΤΑΣΗΣ ΒΕΛΤΙΩΣΗΣ:** | |
| **Περιγραφή:** |  | | | **§ Προδιαγραφής/ Προτύπου:** |
| **Διερεύνηση Αιτιών Εμφάνισης** |  | | | |
| **Διόρθωση/**  **Διορθωτική Ενέργεια** |  | | | **ΗΜΕΡΟΜΗΝΙΑ ΟΛΟΚΛΗΡΩΣΗΣ:** |
| **Α/Α ΜΗ ΣΥΜΜΟΡΦΩΣΗΣ:** | | **Α/Α ΠΑΡΑΤΗΡΗΣΗΣ:** | **Α/Α ΠΡΟΤΑΣΗΣ ΒΕΛΤΙΩΣΗΣ:** | |
| **Περιγραφή:** |  | | | **§ Προδιαγραφής/ Προτύπου:** |
| **Διερεύνηση Αιτιών Εμφάνισης** |  | | | |
| **Διόρθωση/**  **Διορθωτική Ενέργεια** |  | | | **ΗΜΕΡΟΜΗΝΙΑ ΟΛΟΚΛΗΡΩΣΗΣ:** |
| **Α/Α ΜΗ ΣΥΜΜΟΡΦΩΣΗΣ:** | | **Α/Α ΠΑΡΑΤΗΡΗΣΗΣ:** | **Α/Α ΠΡΟΤΑΣΗΣ ΒΕΛΤΙΩΣΗΣ:** | |
| **Περιγραφή:** |  | | | **§ Προδιαγραφής/ Προτύπου:** |
| **Διερεύνηση Αιτιών Εμφάνισης** |  | | | |
| **Διόρθωση/**  **Διορθωτική Ενέργεια** |  | | | **ΗΜΕΡΟΜΗΝΙΑ ΟΛΟΚΛΗΡΩΣΗΣ:** |
| **Α/Α ΜΗ ΣΥΜΜΟΡΦΩΣΗΣ:** | | **Α/Α ΠΑΡΑΤΗΡΗΣΗΣ:** | **Α/Α ΠΡΟΤΑΣΗΣ ΒΕΛΤΙΩΣΗΣ:** | |
| **Περιγραφή:** |  | | | **§ Προδιαγραφής/ Προτύπου:** |
| **Διερεύνηση Αιτιών Εμφάνισης** |  | | | |
| **Διόρθωση/**  **Διορθωτική Ενέργεια** |  | | | **ΗΜΕΡΟΜΗΝΙΑ ΟΛΟΚΛΗΡΩΣΗΣ:** |
| **Α/Α ΜΗ ΣΥΜΜΟΡΦΩΣΗΣ:** | | **Α/Α ΠΑΡΑΤΗΡΗΣΗΣ:** | **Α/Α ΠΡΟΤΑΣΗΣ ΒΕΛΤΙΩΣΗΣ:** | |
| **Περιγραφή:** |  | | | **§ Προδιαγραφής/ Προτύπου:** |
| **Διερεύνηση Αιτιών Εμφάνισης** |  | | | |
| **Διόρθωση/**  **Διορθωτική Ενέργεια** |  | | | **ΗΜΕΡΟΜΗΝΙΑ ΟΛΟΚΛΗΡΩΣΗΣ:** |

|  |  |  |
| --- | --- | --- |
| **ΣΥΜΠΛΗΡΩΘΗΚΕ ΑΠΟ:**  Επικεφαλής Επιθεωρητής | **Υπογραφή** | **Ημερομηνία:** |
| **ΑΠΟΔΟΧΗ ΑΠΟ ΠΕΛΑΤΗ:**  **Έλαβα γνώση της έκθεσης της ομάδας επιθεώρησης και των ευρημάτων** | **Υπογραφή και Σφραγίδα Πελάτη** | **Ημερομηνία:** |

1. Για τη περίπτωση των μη συμμορφώσεων που εντοπίζονται κατά τη διάρκεια της αρχικής επιθεώρησης ή της επαναπιστοποίησης δίνεται ένα χρονικό διάστημα τριών μηνών για την αποκατάσταση τους, ενώ στις περιπτώσεις επιτήρησης το χρονικό διάστημα περιορίζεται στους δύο μήνες. Η αποτελεσματικότητα των ενεργειών που αφορά τις παρατηρήσεις κρίνεται στην επόμενη χρονικά επιθεώρηση.
2. Διενεργείται Εναρκτήρια και Καταληκτική Συνεδρία και ο εντεταλμένος εκπρόσωπος της Διοίκησης λαμβάνει αντίγραφο της παρούσας Αναφοράς Σταδίου 2.
3. Ο υπό επιθεώρηση Οργανισμός βρίσκεται σε λειτουργία και ελέγχεται το αιτούμενο πεδίο εφαρμογής της πιστοποίησης.
4. Τα μέλη της ομάδας επιθεώρησης δεν έχουν καμιά επαγγελματική ή άλλου είδους σχέση με τον επιθεωρούμενο οργανισμό τουλάχιστον για τα τελευταία δυο έτη.
5. Η επιθεώρηση είναι δειγματοληπτικού χαρακτήρα και ως εκ τούτου η μη καταγραφή αρνητικών ευρημάτων ενέχει βαθμό αβεβαιότητας χωρίς να σημαίνει ότι δεν υφίστανται αποκλίσεις στο εφαρμοζόμενο ΣΔΑΠ.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ΕΛΕΓΧΟΣ ΑΝΑΦΟΡΑΣ - ΑΠΟΦΑΣΗ ΧΟΡΗΓΗΣΗΣ / ΔΙΑΤΗΡΗΣΗΣ** | | | | | | |
| Συμπληρώνεται από την Τεχνική Διεύθυνση | | | | | | |
| **ΕΑ / TΠ:** |  | **NACE:** | |  | **Κατηγορία:** |  |
| **Risk:** |  | **Complexity of env. aspects.:** | |  | **Complexity of OH&S risk** |  |
|  | | | | | | |
| **Περιγραφή μεταβολής πεδίου:** | |  | | |  |  |
| **ΠΕΔΙΟ ΠΙΣΤΟΠΟΙΗΣΗΣ (εφόσον υπάρχει μεταβολή):** | | | | | | |
|  | | | | | | |
|
| **ΕΛΕΓΧΟΣ ΔΙΟΡΘΩΤΙΚΩΝ ΕΝΕΡΓΕΙΩΝ** | | | | | | |
| **Ημ/νία Ελέγχου/Αποδοχής ΔΕ:** | |  |  | | **Επάρκεια ΔΕ:** | **Επαρκής** |
| **Υπεύθυνος Ελέγχου ΔΕ:** | |  |  | | **Κατάσταση αναφοράς:** | **Κλειστό** |
| **Σχόλια:**  (σε περίπτωση Επαναπιστοποίησης περιλαμβάνονται και σχόλια για τη συνολική επίδοση του οργανισμού κατά το προηγούμενο κύκλο πιστ/σης) | | | | | | |
| **Σχόλια προς άμεση απάντηση/ διευκρίνηση από Επιθεωρητή προ της Χορήγησης :** | | | | | | |
|  | | | | | | |
| **Παρατηρήσεις:** | | | | | | |
| **Σημεία προς εξέταση κατά την επόμενη επιθεώρηση:** | | | | | | |
|  | | | | | | |
| **Επισημάνσεις / Υποδείξεις για Βελτίωση / Αιτιολόγηση Μη Χορήγησης:** | | | | | | |
| **Α/Η επόμενης επιθεώρησης:** | | | | | | |
| **ΑΠΟΦΑΣΗ ΠΙΣΤΟΠΟΙΗΣΗΣ Ή ΔΙΑΤΗΡΗΣΗΣ** | **ΧΟΡΗΓΗΣΗ** |  | **ΑΝΑΦΟΡΑ ΕΠΙΘΕΩΡΗΣΗΣ:** | | **ΙΚΑΝΟΠΟΙΗΤΙΚΗ** | Έκδοση για τριετία |
| **Υπεύθυνος Χορήγησης ή Ελέγχου:** |  | **Ημ/νία Ελέγχου Αναφοράς & έκδοσης:** |  | | **Ημ/νία έναρξης ισχύος πιστοποίησης:** |  |
| *\*ΥΠΕΥΘΥΝΟΣ ΕΛΕΓΧΟΥ ΑΡΣΗΣ ΜΣ ΚΑΙ ΕΠΑΡΚΕΙΑΣ ΔΕ ΕΙΝΑΙ Ο ΕΠΙΚΕΦΑΛΗΣ ΕΠΙΘΕΩΡΗΤΗΣ ή Ο ΤΕΧΝΙΚΟΣ ΔΙΕΥΘΥΝΤΗΣ* | | | | |  |  |