ΚΑΤΕΥΘΥΝΤΗΡΙΑ ΟΔΗΓΙΑ ΓΙΑ ΤΗ ΔΙΑΠΙΣΤΕΥΣΗ ΦΟΡΕΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ ΣΥΣΤΗΜΑΤΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ (ISMS)

ΕΣΥΔ ΚΟ-ISMS

Έκδοση: 01
Αναθεώρηση: 00
Ημερομηνία αρχικής έκδοσης: 29-03-2006
Ημερομηνία αναθεώρησης:
Υπεύθυνος Σύνταξης: ΟΥπεύθυνος Διαχείρισης της Ποιότητας
Υπεύθυνος Έγκρισης: Ο Πρόεδρος του Ε.ΣΥ.Δ.

Ο Υπεύθυνος Διαχείρισης Ποιότητας **Ο Πρόεδρος του Ε.ΣΥ.Δ.**

Κατά την αξιολόγηση και τη διαπίστευση από το ΕΣΥΔ φορέων πιστοποίησης συστημάτων διαχείρισης της ασφάλειας πληροφοριών (ISMS), ισχύουν οι παρακάτω απαιτήσεις.

- Το Πρότυπο, ως προς το οποίο θα διενεργείται η πιστοποίηση ενός συστήματος ISMS είναι το Πρότυπο ISO/IEC 27001:2005 και ενδεχομένως πλαισιωμένο από σχετικά τυποποιητικά έγγραφα.

- Η επάρκεια των Φορέων Πιστοποίησης ως προς το Πρότυπο αυτό αξιολογείται με βάση την ΕΑ-7/03.

Ο Φορέας Πιστοποίησης οφείλει :

- Να διαθέτει τεκμηριωμένη γνώση των προτύπων ή των άλλων τυποποιητικών εγγράφων, των μεθόδων δοκιμής και ελέγχου της ασφάλειας πληροφοριών, καθώς και γνώση του επιμέρους βιομηχανικού τομέα, επί του οποίου εφαρμόζεται το ISMS.

- Να αναγνωρίζει τις ανάγκες εκπαίδευσης των επιθεωρητών του και να παρέχει εκπαίδευση για την ικανοποίηση των αναγκών αυτών. Οι ανάγκες εκπαίδευσης πρέπει να επανεξετάζονται σε τακτά διαστήματα. Πρέπει να τηρούνται αρχεία εκπαίδευσης που να τεκμηριώνουν την ικανοποίηση των παραπάνω αναγκών.

- Να παρακολουθεί τις απαιτήσεις της νομοθεσίας και του κανονιστικού πλαισίου πού διέπει την δραστηριοποίηση στον χώρο των συστημάτων πληροφορικής και επικοινωνιών σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο και ιδιαίτερα εκείνες που αφορούν την προστασία από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και το απόρρητο των επικοινωνιών. Ο Φορέας Πιστοποίησης ο οποίος πιστοποιεί συστήματα ISMS οργανισμών οι οποίοι εμπίπτουν στις περιπτώσεις του Παρατήματος Α πρέπει να λαμβάνει επιπλέον υπόψιν τις απαιτήσεις του Παρατήματος αυτού.

- Να είναι ενήμερος του νομικού και κανονιστικού πλαισίου που διέπει τις υπηρεσίες ψηφιακών υπογραφών καθώς και των συστημάτων που τις υλοποιούν όταν και εφόσον αυτά τεθούν σε λειτουργία σύμφωνα με την ισχύουσα νομοθεσία.

Τα μέλη της ομάδας επιθεώρησης οφείλουν να διαθέτουν, μεταξύ των άλλων:

- Τεκμηριωμένη γνώση των νομικών απαιτήσεων που ισχύουν για τα υπό πιστοποίηση συστήματα.
- Επάρκεια των τεχνικών γνώσεων η οποία αποδεικνύεται με πτυχίο ή δίπλωμα πανεπιστημιακού επιπέδου, ειδικότητας συναφούς με τον κλάδο της ασφάλειας πληροφοριών και συστημάτων όπως πληροφορικής, υπολογιστών και μαθηματικών.

ΠΑΡΑΡΤΗΜΑ Α:

Χ. Πιστοποίηση/καταχώρηση οργανισμών που ενεργοποιούνται ως πάροχοι επικοινωνιακών και διαδικτυακών υπηρεσιών

Χ.1 Ο φορέας πιστοποίησης θα πρέπει να ελέγχει ότι *οργανισμός,* ο οποίος ενεργοποιείται ως πάροχος επικοινωνιακών και διαδικτυακών υπηρεσιών,

(α) έχει αδειοδοτηθεί από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων – ΕΕΤ.

(β) έχει ανταποκριθεί με κατάλληλες διορθωτικές ενέργειες μετά από παρατηρήσεις ή κυρώσεις από την πλευρά της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Χ.2 Ο φορέας πιστοποίησης θα πρέπει να ελέγχει ότι *οργανισμός,* ο οποίος ενεργοποιείται ως πάροχος επικοινωνιακών και διαδικτυακών υπηρεσιών, παρουσιάζει ανάλογα με του τομείς δραστηριοποίησής του τεκμηριωμένη Πολιτική Διασφάλισης του Απορρήτου των Τηλεπικοινωνιακών Υπηρεσιών ή Πολιτική Ασφάλειας Υποδομών, Επικοινωνιών, Υπηρεσιών ή Εφαρμογών, όπως αυτές ζητούνται από τις Αποφάσεις της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών – ΑΔΑΕ, και ειδικότερα για παρόχους

(α) κινητών τηλεπικοινωνιακών υπηρεσιών, από την Απόφαση 629α, Άρθρο 3, ΦΕΚ 87/26.01.05.

(β) σταθερών τηλεπικοινωνιακών υπηρεσιών, από την Απόφαση 630α, Άρθρο 3, ΦΕΚ 87/26.01.05.

(γ) τηλεπικοινωνιακών υπηρεσιών μέσω ασυρμάτων δικτύων, από την Απόφαση 631α, Άρθρο 3, ΦΕΚ 87/26.01.05.

(δ) διαδικτυακών υπηρεσιών, υπηρεσιών πρόσβασης στο διαδίκτυο και διαδικτυακών υπηρεσιών προστιθεμένης αξίας, από το Άρθρο 3 των Αποφάσεων, κατά περίπτωση, 632α, 633α, ή 634α του ΦΕΚ 88/26.01.05.

Ο *οργανισμός* θα πρέπει να έχει διαθέσιμα όλα τα στοιχεία τα σχετικά με την διαδικασία έγκρισης και ελέγχου εφαρμογής της παραπάνω πολιτικής από την ΑΔΑΕ, σε οποιοδήποτε στάδιο και αν ευρίσκεται η έγκριση ή έλεγχος εφαρμογής της πολιτικής αυτής.

Υ. Πιστοποίηση/καταχώρηση τραπεζικών οργανισμών

Υ.1 Ο φορέας πιστοποίησης θα πρέπει να ελέγχει ότι *τραπεζικός οργανισμός,* του οποίου το πιστοποιούμενο ISMS περιλαμβάνει αυτόματες ταμειολογικές μηχανές (ΑΤΜ), παρουσιάζει τεκμηριωμένο Προγραμματισμό Επιβολής Μέτρων Προστασίας, όπως αυτός ζητείται από την Απόφαση ΑΔΑΕ 969, ΦΕΚ 298/08.03.05 της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), που αφορά στην «Διασφάλιση Απορρήτου κατά τη Χρήση Αυτομάτων Ταμειολογικών Μηχανών».