ISMS κατά ISO 27001

Δεκέμβριος 2016

Κουντουριώτη 21, Θεσσαλονίκη, Τηλ: 2310-541017,Fax: 2310-521402,Τ.Κ:54625,
E-mail: info@motive.com.gr, Web: www.motive.com.gr

ISO 27001:2013

Το ISO 27001:2013 είναι ένα διεθνώς αναγνωρισμένο πρότυπο το οποίο προσδιορίζει τις προδιαγραφές για την διαχείριση της ασφάλειας των πληροφοριών.

Μπορεί να χρησιμοποιηθεί από εταιρίες, που επιθυμούν να εγκαταστήσουν και να βελτιώσουν την ασφαλή διαχείριση των δεδομένων τους και των πελατών τους.

Ανάπτυξη Συστήματος Διαχείρισης Ποιότητας – Ασφάλεια των Πληροφοριών κατά ISO/IEC 27001

Σκοπός του ISO / IEC 27001: 2013, είναι να εξασφαλίσει την ύπαρξη επαρκών και κατάλληλων ελέγχων, σε θέματα εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας της πληροφορίας, προστατεύοντας έτσι τα δεδομένα των ενδιαφερόμενων μερών. Τα ενδιαφερόμενα μέρη στα οποία απευθύνεται μπορεί να είναι πελάτες, οργανισμοί και επιχειρήσεις, προσωπικό, συνεργάτες αλλά και η κοινωνία γενικότερα.

Τόσο η προστασία προσωπικών δεδομένων όσο και η αντιμετώπιση κινδύνων που σχετίζονται με την ανεπάρκεια ή δυσλειτουργία συστημάτων IT, αποτελούν θέματα υψίστης σημασίας για οργανισμούς και επιχειρήσεις.

Το ISO / IEC 27001: 2013 αποτελεί την νέα προδιαγραφή για την Διαχείριση της Ασφάλειας των Πληροφοριών και έχει εφαρμογή σε όλους τους κλάδους που δραστηριοποιούνται σε βιομηχανία, εμπόριο και παροχή υπηρεσιών.

Κουντουριώτη 21, Θεσσαλονίκη, Τηλ: 2310-541017,Fax: 2310-521402,Τ.Κ:54625,
E-mail: info@motive.com.gr, Web: www.motive.com.gr

Οφέλη της επιχείρησης με την χρήση του ISO / IEC 27001: 2013

- **Μείωση επιχειρηματικού ρίσκου και κόστους** – Εξασφαλίζει την ύπαρξη ελέγχων τόσο για την μείωση του ρίσκου όσο και για την αποφυγή εκμετάλλευσης τυχόν αδυναμιών του συστήματος. Ακόμα και αν το χειρότερο συμβεί, ο οργανισμός είναι σε θέση να το αντιμετωπίσει και να ανακτήσει τον έλεγχο το συντομότερο δυνατό.
- **Βέλτιστη Πρακτική** – Διασφάλιση ότι υπάρχει δέσμευση ως προς την ασφάλεια πληροφοριών από όλους και σε όλα τα επίπεδα του οργανισμού.
- **Συμμόρφωση με νομικές και κανονιστικές απαιτήσεις**
- **Ανταγωνιστικότητα** - Τόνωση και προβολή της εμπορικής εικόνας. Αύξηση της εμπιστοσύνης των πελατών, συνεργατών και γενικά όλων των ενδιαφερόμενων μερών, με την επίγνωση ότι η διαχείριση των πληροφοριών και των δεδομένων τους είναι ασφαλής.
- **Ενιαίο Σύστημα Διαχείρισης** – Βασισμένο στον κύκλο « Σχεδιάζω – εκτελώ – ελέγχω – ενεργώ» το ISO / IEC 27001: 2013 έχει αρκετά κοινά με άλλα πρότυπα όπως 9001 και 14001, καθιστώντας ευκολότερη την ανάπτυξη ενός ενιαίου

συστήματος διαχείρισης που ικανοποιεί τις απαιτήσεις και άλλων προτύπων αποφεύγοντας έτσι επαναλήψεις και περιττά κόστη.

Οι απαιτήσεις του προτύπου είναι λογικές και στις περισσότερες περιπτώσεις αυτονόητες, όπως:

- προδιαγραφές για υλικά, προϊόντα και υπηρεσίες
- μέθοδοι ανταπόκρισης του οργανισμού για τις δεσμεύσεις και προδιαγραφές που δίνει στους πελάτες
- οργανόγραμμα, υπευθυνότητες, αρμοδιότητες (ποιος κάνει τι, με τι εξουσιοδότηση)
- σχεδιασμένες διαδικασίες για τις κρίσιμες ή πολύπλοκες λειτουργίες
- καθορισμένος τρόπος επικοινωνίας και διαχείρισης των πληροφοριών
- συγκεκριμένοι στόχοι για τη συνεχή βελτίωση του οργανισμού
- διαδικασίες ελέγχου και αξιολόγησης των δεδομένων, των μεθόδων και των ανθρώπων
- Καταγραφή όλων των χρήσιμων και κρίσιμων δεδομένων που χρειάζεται ο οργανισμός για να διασφαλίζει τη καλή λειτουργία του και να χτίζει τη βελτίωσή του.

ΠΑΡΑΡΤΗΜΑ Ι

Το πρότυπο περιέχει 10 θεματικές ενότητες, οι οποίες εξετάζουν τις βασικές περιοχές διαχείρισης πληροφοριών:

Α/Α	Θεματική Ενότητα	
1	**Information Security Policy**	Λεπτομερής κατανόηση των επιχειρησιακών στόχων της εταιρίας και δημιουργία της κατάλληλης πολιτικής ασφάλειας των πληροφοριών.
2	**Information Security Infrastructure**	Διαμόρφωση ενός διοικητικού πλαισίου το οποίο χρειάζεται για να αρχίσει να εφαρμόζεται και να ελέγχεται η ασφάλεια των πληροφοριών μέσα στην εταιρία.

3	**Asset classification and control**	Λεπτομερής καταγραφή των εταιρικών πόρων της εταιρίας και προσδιορισμός του επιπέδου ασφάλειας που απαιτείται για τους πόρους αυτούς.
4	**Personnel Security**	Μείωση κινδύνων από ανθρώπινο σφάλμα, κλοπή, απάτη ή κακή χρήση των εταιρικών πόρων, καθώς και διασφάλιση ότι το προσωπικό γνωρίζει την πολιτική ασφάλειας των πληροφοριών και την εφαρμόζει στην καθημερινή εργασία του.
5	**Physical and Environmental Security**	Αποτροπή της αναρμόδιας πρόσβασης, της ζημία και της παρέμβασης στις επιχειρησιακές εγκαταστάσεις και τις πληροφορίες καθώς τυχόν απώλειας, ζημίας ή και διακοπής στις δραστηριότητες της επιχείρησης.
6	**Computer & Network Management**	Εξασφάλιση της σωστής και ασφαλούς λειτουργίας των δυνατοτήτων επεξεργασίας πληροφοριών, ελαχιστοποίηση κινδύνου να τεθούν τα συστήματα πληροφορικής εκτός λειτουργίας, προστασία της ακεραιότητας του λογισμικού και των πληροφοριών, εξασφάλιση της προστασίας των πληροφοριών στα δίκτυα και τη σχετική υποδομή.
7	**Access Control**	Έλεγχος πρόσβασης στις πληροφορίες, εξασφάλιση προστασίας των δικτύων, αποτροπή αναρμόδιας πρόσβασης σε υπολογιστές, ανίχνευση αναρμόδιων δραστηριοτήτων.
8	**System Development & Maintenance**	Η ενότητα αυτή έχει στόχο να εξασφαλίσει ότι η αναγκαία ασφάλεια εμπεριέχεται στα λειτουργικά σύστηματα, να αποτρέψει την απώλεια, την τροποποίηση ή την κακή χρήση των στοιχείων χρηστών εφαρμογών, να εξασφαλίσει ότι τα προγράμματα και οι δραστηριότητες υποστήριξης διευθύνονται με έναν ασφαλή τρόπο.
9	**Business Continuity Planning**	Διαμόρφωση τρόπου αντίδρασης σε διακοπές επιχειρησιακών δραστηριοτήτων και κρίσιμων επιχειρησιακών διαδικασιών που είναι αποτελέσματα σημαντικών αποτυχιών ή καταστροφών.
10	**Compliance**	Αποφυγή παραβιάσεων εγκληματικού ή αστικού δικαίου, νομικών, ρυθμιστικών ή συμβατικών υποχρεώσεων και οποιωνδήποτε απαιτήσεων ασφάλειας.