

ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

βάση του προτύπου ISO/IEC 27001:2005



Η πληροφορία που παράγει ή διαχειρίζεται ένας οργανισμός κατά την λειτουργία του, είναι ένα αντικείμενο ζωτικής σημασίας. Σήμερα, οι πληροφορίες θεωρούνται ως προϊόντα με επιχειρησιακή αξία, χρησιμότητα και σημασία. Αξίζει να σημειωθεί πως αυτό ισχύει για όλα τα είδη και μεγέθη των επιχειρήσεων. Για τον λόγο αυτό η αναγνώριση της επιχειρησιακής αξίας των πληροφοριών είναι μέγιστης σπουδαιότητας σε όλους τους οργανισμούς.

Η πληροφορία λαμβάνει διάφορες μορφές όπως, έντυπη ή χειρόγραφη σε χαρτί, σε ηλεκτρονική μορφή, αποθηκευμένη σε συστήματα υπολογιστών, σε βάσεις δεδομένων ή διακινούμενη σε δίκτυα κάθε είδους, μέσω ηλεκτρονικού ταχυδρομείου ή άλλων υπηρεσιών. Επίσης η πληροφορία μπορεί να επιδεικνύεται σε παρουσιάσεις με διάφορα οπτικά μέσα, ή ακόμη να παράγεται σε προφορική μορφή κατά την διάρκεια συζητήσεων ή τηλεφωνικών συνδιαλέξεων.

Δεδομένου ότι οι πληροφορίες αυξάνονται στον όγκο, την πολυπλοκότητα, και την κρισιμότητά τους, και καθώς η πρόσβαση στις πληροφορίες διευρύνεται, είναι όλο και περισσότερο τρωτές. Περισσότεροι άνθρωποι μπορούν να έχουν πρόσβαση σε περισσότερα στοιχεία όσο ποτέ άλλοτε. Συνεπώς η ασφάλεια των ευαίσθητων πληροφοριών επιχείρησης καθίσταται μια απόλυτη ανάγκη για τους οργανισμούς.

Οι διάφοροι τύποι απειλών, αδυναμιών και ρίσκου που αντιμετωπίζουν οι επιχειρήσεις σε καθημερινή βάση προκαλούν τεράστιες ανησυχίες, και έχει γίνει προφανές ότι ένα σύστημα που να διαχειρίζεται την ασφάλεια πληροφοριών θεωρείται απολύτως αναγκαίο. Χωρίς ασφάλεια πληροφοριών, η επιχείρηση βρίσκεται αντιμέτωπη με τις διάφορες αρνητικές επιδράσεις συμπεριλαμβανομένων των οικονομικών συνεπειών, αδυναμίας στην προστασία της πνευματικής ιδιοκτησίας του οργανισμού, της απώλειας μεριδίου αγοράς, της μειωμένης παραγωγικότητας και απόδοσης, των ατελέσφορων διαδικασιών, της ανικανότητας να συμμορφωθεί με τους νόμους και τους κανονισμούς, ή ακόμη και της απώλειας φήμης.

Για τον σκοπό αυτό απαιτείται η ανάπτυξη και ενσωμάτωση στην λειτουργία του οργανισμού, ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System-ISMS) συνιστά μια συνολική και συστηματική προσέγγιση του οργανισμού στην διαχείριση της ευαίσθητης πληροφορίας του και των κινδύνων που την απειλούν, έτσι ώστε η πληροφορία να παραμένει ασφαλής. Η ασφάλεια της πληροφορίας βασίζεται στα εξής τρία στοιχεία:

- **ακεραιότητα:** οι πληροφορίες είναι πλήρεις και αδιάφθορες.
- **διαθεσιμότητα:** οι πληροφορίες είναι προσιτές σε εκείνους που τις χρειάζονται.
- **εμπιστευτικότητα:** οι πληροφορίες είναι ασφαλείς από την πρόσβαση μη-εξουσιοδοτημένων ατόμων.

Ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών είναι ένα σύστημα διοίκησης που επιδρά στο σύνολο του οργανισμού και περιλαμβάνει το προσωπικό, τις διαδικασίες και τα συστήματα πληροφορικής του οργανισμού. Επίσης, ένα τέτοιο σύστημα μπορεί να ενσωματωθεί σε οργανισμούς κάθε είδους, μεγέθους, ή επιχειρησιακού κλάδου. Από αυτή την άποψη, ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών εμφανίζει αρκετές ομοιότητες με ένα Σύστημα Διαχείρισης Ποιότητας. Σε πολλές περιπτώσεις ένας οργανισμός αναπτύσσει ταυτόχρονα και συνδυασμένα, το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών μαζί με το Σύστημα Διαχείρισης Ποιότητας(ISO 9001:2000).

Συνοπτικά τα ωφέλη για έναν οργανισμό από την υιοθέτηση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών είναι σημαντικά και πολλαπλά. Ενδεικτικά αναφέρονται τα εξής:

- αποδεικνύει τη συμμόρφωση με τις απαιτήσεις του προτύπου ISO/IEC 27001:2005.
- παροχή διαβεβαίωσης στους διευθυντές και στα ενδιαφερόμενα μέρη ότι η επιχείρηση συμμορφώνεται με την υπάρχουσα νομοθεσία.
- βελτιώνει την αξιοπιστία και ενισχύει την εμπιστοσύνη πελατών.
- αποδεικνύει τη δέσμευση της ανώτερης διοίκησης για την ασφάλεια των πληροφοριών ενός οργανισμού.
- δέσμευση του προσωπικού και βελτίωση της κουλτούρας ασφάλειας των πληροφοριών στην εργασία.
- παρέχει την ευκαιρία για τη συνεχή βελτίωση μέσω των συστηματικών επιθεωρήσεων.
- εξασφάλιση της αποτελεσματικής ολοκλήρωσης των θεμάτων διαχείρισης της ασφάλειας των πληροφοριών με άλλα διαχειριστικά συστήματα (π.χ. ISO 9001:2000).
- μείωση του κόστους - από άμεσα κόστη π.χ. κλοπή φορητού υπολογιστή, και από έμμεσα κόστη π.χ. φήμη, νομικές απώλειες.
- παροχή ανταγωνιστικού πλεονεκτήματος και αναβάθμιση της εικόνας του Οργανισμού

Για την ανάπτυξη και εφαρμογή Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών, υπάρχουν δύο αλληλοσυμπληρούμενα πρότυπα,

- ISO/IEC 27001:2005 "Information Security Management Systems - Requirements"
- ISO/IEC 17799:2005 "Code of practice for information security management"

τα οποία μελλοντικά θα αποτελέσουν την σειρά προτύπων ISO/IEC 27000 και έχουν αναπτυχθεί από τον Διεθνή Οργανισμό Τυποποίησης (ISO) και συγκεκριμένα την Τεχνική Επιτροπή ISO/IEC JTC1 SC27.



Μετά την ανάπτυξη και εφαρμογή στον οργανισμό του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ακολουθεί η φάση της πιστοποίησης του συστήματος κατά το πρότυπο ISO/IEC 27001:2005. Η πιστοποίηση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ενός οργανισμού κατά ISO/IEC 27001:2005 πραγματοποιείται από Οργανισμούς Πιστοποίησης (certification bodies) δηλαδή ανεξάρτητους φορείς αναγνωρισμένου κύρους με διαπιστευμένη ικανότητα πιστοποίησης Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών.

Η πιστοποίηση του συστήματος διαχείρισης ασφάλειας πληροφοριών ενός οργανισμού είναι ένας τρόπος διαβεβαίωσης ότι ο πιστοποιημένος οργανισμός έχει εφαρμόσει ένα σύστημα για τη διαχείριση της ασφάλειας πληροφοριών σύμφωνα με τις απαιτήσεις του ISO/IEC 27001:2005.

Η **Κυπριακή Εταιρεία Πιστοποίησης (Κ.Ε.Π)**, ο πλέον εδραιωμένος φορέας πιστοποίησης στην Κύπρο προσφέρει τις υπηρεσίες της τώρα και στον τομέα της Πιστοποίησης Συστημάτων Διαχείρισης Ασφάλειας Δεδομένων (ISMS) μέσω της συνεργασίας της με τον καταξιωμένο Οργανισμό Πιστοποίησης "**Certification International (UK)**", που δραστηριοποιείται τόσο στον Ευρωπαϊκό όσο και στο διεθνή χώρο.

Την παρούσα στιγμή έχουν εγγραφεί περισσότερες από 2800 πιστοποιημένες εταιρείες σε παγκόσμιο επίπεδο. Για περισσότερες πληροφορίες για το χώρο της πιστοποίησης ISMS μπορείτε να επισκεφθείτε την ιστοσελίδα www.iso27001certificates.com.

Διαμαντής Ζαφειριάδης
Λειτουργός Τυποποίησης του
Κυπριακού Οργανισμού Τυποποίησης (CYS)