Γιατί ασφάλεια **πληροφοριών**;
Η σημασία της πληροφορίας στην ασφάλεια.
Το πληροφοριακό σύστημα σαν το μέσο επεξεργασίας και αποθήκευσης.
Συχνά αποσκοπούμε λανθασμένα να προστατεύσουμε το πληροφοριακό σύστημα και όχι την πληροφορία αυτή καθεαυτή.
Η αποσπασματική προστασία του πληροφοριακού συστήματος συχνά δε μπορεί να προστατεύσει αποτελεσματικά την ίδια την πληροφορία.

Τι ονομάζουμε διαχείριση της ασφάλειας πληροφοριών; Γιατί τη χρειαζόμαστε;

Η διαχείριση της ασφάλειας πληροφοριών στοχεύει στην προστασία των πληροφοριακών συστημάτων, περιορίζοντας την επικινδυνότητα σε αποδεκτό επίπεδο.
Περιλαμβάνει συνοπτικά :
•Αξιολόγηση της επικινδυνότητας και προσδιορισμό του αποδεκτού επιπέδου ασφάλειας
•Ανάπτυξη και εφαρμογή μιας Πολιτικής Ασφάλειας
•Δημιουργία κατάλληλου οργανωτικού πλαισίου και εξασφάλιση των απαιτούμενων πόρων για την εφαρμογή της Πολιτικής Ασφάλειας.
•Εκπαίδευση, ενημέρωση και ευαισθητοποίηση των χρηστών των ΠΣ για ζητήματα ασφάλειας

Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών

Η χρήση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System - ISMS) στοχεύει στη συστηματική διατήρηση της:
•Διαθεσιμότητας
•Εμπιστευτικότητας
•Ακεραιότητας
των πληροφοριών και των πληροφοριακών συστημάτων ενός οργανισμού.

Κίνδυνοι πληροφοριών
Όλα τα πληροφοριακά συστήματα έχουν ευπάθειες που μπορούν να τύχουν εκμετάλλευσης από απειλές με σημαντικές συνέπειες στη λειτουργία ενός οργανισμό, τη κερδοφορία, αξία και μακροπρόθεσμη επιβίωσή του.

Περιλαμβάνουν επίσης έννοιες όπως:
•Αυθεντικότητα
•Υπευθυνότητα
•Μη αποποίηση
•Αξιοπιστία

Εξωτερικές απειλές:
Ιοί, σκουλήκια, δούρειοι ίπποι
Hackers – χρησιμοποιώντας αυτοματοποιημένες επιθέσεις
Spam
Οργανωμένο έγκλημα – phishing, κλοπή ταυτότητας
Απάτη, ψηφιακή τρομοκρατία
Ανταγωνισμός
Ακτιβιστές
Πρακτικά οποιοσδήποτε έχει υπολογιστή!

Εσωτερικές απειλές
Απάτες, λάθη, μη εξουσιοδοτημένη ή παράνομη χρήση συστημάτων, κλοπή δεδομένων
system use, data theft

Ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) διασφαλίζει έναν οργανισμό από αυτές τις απειλές (εσωτερικές-εξωτερικές)

2005: ISO 27001

2000: ISO 17799

1998: BS7799 p.2

1995: BS7799

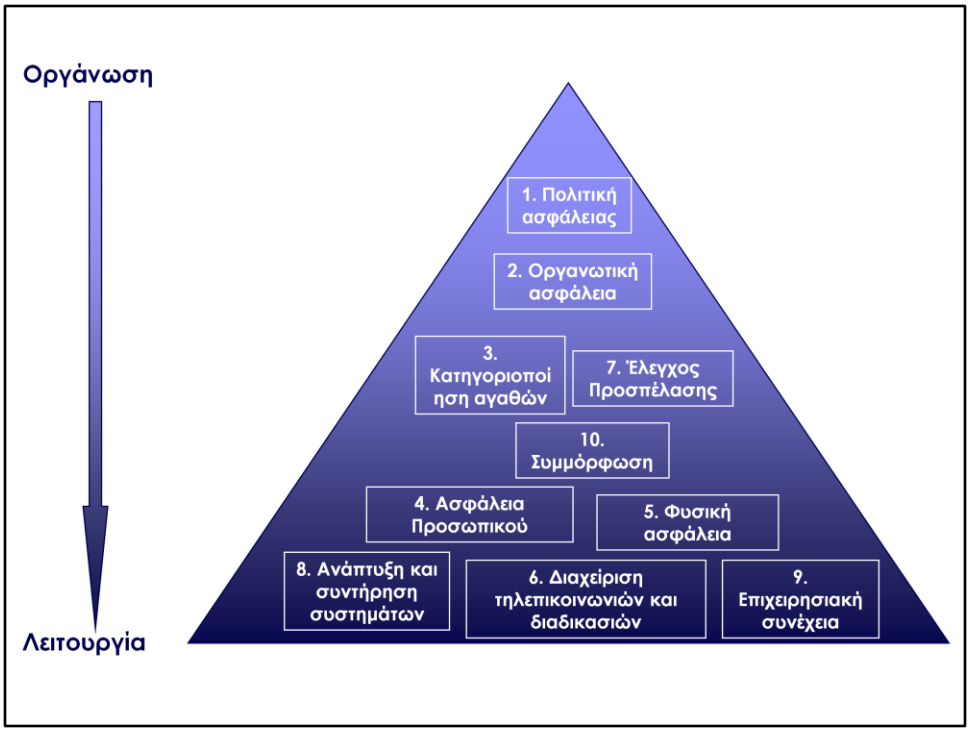
ISO 27001: περιγράφει τις προδιαγραφές δημιουργίας ενός Συστήματος Διαχείρισης της Ασφάλειας Πληροφοριών
Ανήκει στην οικογένεια ISO 27000

Ιστορικό:

1995	BS 7799 Part 1
1998	BS 7799 Part 2
1999	Updated version of BS 7799 Parts 1 and 2
2000	ISO/IEC 17799:2000
2001	Review of BS 7799-2
2002	BS7799-2
2005	ISO 17799 ISO 27001

Γιατί να το υιοθετήσει κανείς:
•Ευρύ πεδίο εφαρμογής
•Αποδεδειγμένα αποτελέσματα
•Δημόσια διαθέσιμο
•Διεθνές πρότυπο
•Συνυφασμένο με την «ποιότητα»
•Ευέλικτο (εφαρμόζεται σε κάθε πεδίο)
•Διαθεσιμότητα εργαλείων και υποστήριξης
•Συμμόρφωση με νομοθεσία για διαχείριση των κινδύνων
•Καλύτερη προστασία των εταιρικών εμπιστευτικών πληροφοριών
•Μειωμένοι κίνδυνοι επιθέσεων από hackers
•Γρηγορότερη και ευκολότερη ανάκαμψη από μια επίθεση
•Δομημένη μεθοδολογία που τυγχάνει διεθνούς αναγνώρισης.
•Αμοιβαία εμπιστοσύνη μεταξύ πιστοποιημένων εταίρων
•Βελτιωμένες πρακτικές ιδιωτικότητας
•Εικόνα του οργανισμού: αποδεδειγμένο ενδιαφέρον για την ασφάλεια. Ωφελεί και στην προώθηση-διαφήμιση.

Στην Ελλάδα:
Πριν 5 χρόνια 4 μόνο πιστοποιημένοι οργανισμοί (Vodafone, Encode, Eurobank). Εδώ και 1,5 χρόνο έχουν πιστοποιηθεί πάνω από 30.



Κάλυψη όλου του φάσματος της ασφάλειας σε έναν οργανισμό από την οργάνωση-διοίκηση μέχρι τη λειτουργία του, σε 10 συνολικά περιοχές.

Σημαντικό: Δέσμευση της διοίκησης για εφαρμογή του προτύπου και επιβολή του ΣΔΑΠ

Το ανθρώπινο δυναμικό είναι ίσως το πιο σημαντικό και το πιο κρίσιμο στοιχείο ενός ΣΔΑΠ.

Στόχος: Η διασφάλιση ότι οι υπάλληλοι, τα στελέχη, οι συνεργάτες και τρίτοι αντιλαμβάνονται τις ευθύνες τους και είναι κατάλληλοι για τους ρόλους που τους έχουν ανατεθεί και σε τελική ανάλυση για τη μείωση των κινδύνων πληροφορικής, είτε από ακούσιες είτε από εκούσιες ενέργειες.

Οι ευθύνες όσον αφορά την ασφάλεια θα πρέπει να έχουν διευκρινιστεί πριν την πρόσληψη μέσα από επαρκής περιγραφές της θέσης καθώς και στις αντίστοιχες συμβάσεις πρόσληψης. Όλα τα υποψήφια στελέχη, συνεργάτες και τρίτοι θα πρέπει να ελέγχονται επαρκώς, ειδικά όταν προορίζονται για ευαίσθητες εργασίες, και να υπογράφουν συμφωνητικά εχεμύθειας και ανάληψης των ευθυνών όσων αφορά την ασφάλεια, το ρόλο και τις αρμοδιότητές τους.

Επίσης, θα πρέπει να γνωρίζουν τους κινδύνους ασφάλειας πληροφοριών καθώς και τις αντίστοιχες ευθύνες που προκύπτουν για αυτούς αλλά και τις επιπτώσεις. Θα πρέπει να τηρούν την πολιτική ασφάλειας κατά την καθημερινή τους εργασία και να μειώνουν τους κινδύνους ανθρώπινων λαθών.

Θα πρέπει να ορίζονται οι ευθύνες και οι αρμοδιότητες της διοίκησης ώστε να διασφαλίζεται ότι η πολιτική ασφάλειας εφαρμόζεται σε όλο τον οργανισμό. Επίσης θα πρέπει να διατηρείται ένα επαρκές επίπεδο ευαισθητοποίησης, ενημέρωσης και εκπαίδευσης όσον αφορά τις διαδικασίες ασφάλειας και την ορθή χρήση των πληροφοριακών συστημάτων σε όλο το προσωπικό του οργανισμού, τους συνεργάτες και τρίτους φορείς που χρησιμοποιούν την πληροφοριακή υποδομή.

Θα πρέπει επίσης να υπάρχει μία επίσημη διαδικασία διαχείρισης περιστατικών ασφάλειας.

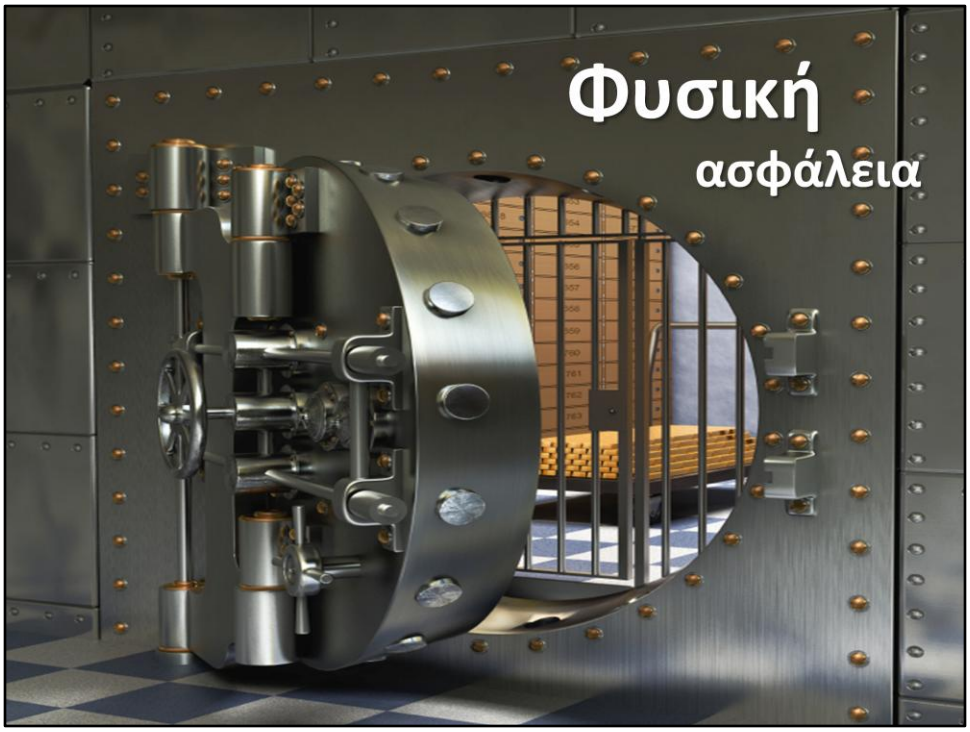
Στόχος: Η επίτευξη και διατήρηση του απαραίτητου επιπέδου προστασίας των επιχειρησιακών αγαθών

•Καταγραφή των πόρων και των αγαθών
•Καθορισμός υπευθύνου για κάθε αγαθό: υπεύθυνος για την υλοποίηση και την παρακολούθηση των μηχανισμών ασφάλειας και ελέγχου (δεν τους υλοποιεί απαραίτητα ο ίδιος αλλά σε κάθε περίπτωση παραμένει υπεύθυνος για τη συνολική προστασία των αγαθών)
•Προσδιορισμός επιτρεπόμενης χρήσης και σκοπού
•Τελική λίστα (inventory) με όλα τα αγαθά.

Αγαθά:
•Πληροφορίες: αρχεία, βάσεις δεδομένων, συμβόλαια, συμφωνίες, εγχειρίδια, διαδικασίες, κλπ.
•Λογισμικό
•Φυσικά αγαθά: υπολογιστές, αποθηκευτικά μέσα
•Υπηρεσίες: πληροφοριακές και τηλεπικοινωνιακές υπηρεσίες, υπηρεσίες κοινής ωφέλειας: θέρμανση, ψύξη, φωτισμός
•Άνθρωποι, ικανότητές τους και εμπειρία τους
•Εταιρική φήμη

Στόχος: Η επίτευξη και διατήρηση του απαραίτητου επιπέδου προστασίας της πληροφορίας.

•Η πληροφορία θα πρέπει να διαβαθμίζεται ώστε να υποδεικνύεται η ανάγκη, προτεραιότητα και αναμενόμενος βαθμός προστασίας της.
•Διαβάθμιση ανάλογα με την αξία της, τις νομικές απαιτήσεις, την ευαισθησία και την κρισιμότητά της.
•Πολλαπλοί βαθμοί ευαισθησίας και κρισιμότητας
•Σχήμα διαβάθμισης. Π.χ.: Αδιαβάθμητο, εμπιστευτικό, απόρρητο, άκρως απόρρητο



Στόχος: Η αποτροπή μη εξουσιοδοτημένης φυσικής πρόσβασης, καταστροφής ή παρεμβολής στην υποδομή και τις πληροφορίες του οργανισμού.
Υποδομές που διαχειρίζονται κρίσιμες ή εμπιστευτικές πληροφορίες θα πρέπει να βρίσκονται σε ασφαλείς περιοχές, προστατευμένες από περιμετρική ασφάλεια με φυσικά εμπόδια και έλεγχο πρόσβασης. Θα πρέπει να προστατεύονται φυσικά από μη εξουσιοδοτημένη πρόσβαση, καταστροφή ή παρεμβολή. Η προστασία που θα παρέχεται θα πρέπει πάντα να είναι αντίστοιχη των κινδύνων που έχουν εντοπιστεί.

Ασφαλείς περιοχές
- Περίμετρος φυσικής ασφάλειας
- Έλεγχοι φυσικής πρόσβασης
- Ασφάλεια γραφείων και χώρων
- Εργασία σε ασφαλείς περιοχές
- Απομονωμένες περιοχές παράδοσης και φόρτωσης

Επίσης θα πρέπει να εφαρμόζονται μέτρα ώστε να αποτρέπεται η απώλεια, καταστροφή, κλοπή ή παραβίαση αγαθών καθώς και η διακοπή της λειτουργίας του οργανισμού.
Για το λόγο αυτό ο εξοπλισμός θα πρέπει να προστατεύεται από φυσικές και περιβαλλοντικές απειλές.

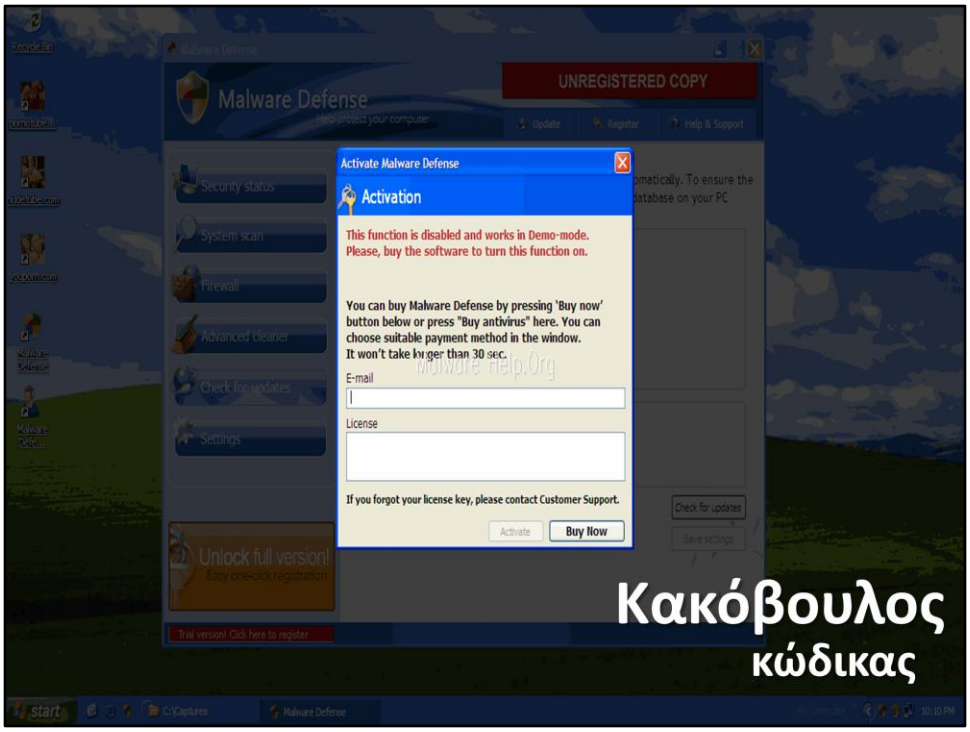
Η προστασία του εξοπλισμού (συμπεριλαμβανομένου αυτού που χρησιμοποιείται εκτός των εγκαταστάσεων του οργανισμού) είναι απαραίτητη για τη μείωση των κινδύνων μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες και για την προστασία από κλοπή ή απώλεια πληροφοριών. Τα μέτρα προστασίας θα πρέπει να συμπεριλαμβάνουν διαδικασίες εγκατάστασης και καταστροφής . Ειδικά μέτρα μπορεί να απαιτούνται για την προστασία από φυσικές απειλές και τη διασφάλιση των αντίστοιχων υποστηρικτικών υποδομών όπως η παροχή ηλεκτρικού ρεύματος, καλωδίωση, κλπ.

Ασφάλεια εξοπλισμού
- Θέση και προστασία εξοπλισμού
- Παροχή ενέργειας
- Ασφάλεια καλωδιώσεων
- Συντήρηση εξοπλισμού
- Ασφάλεια εξοπλισμού εκτός χώρων του οργανισμού
- Ασφαλής απόσυρση εξοπλισμού

Γενικοί έλεγχοι
- Πολιτική καθαρής οθόνης και καθαρού γραφείου: να μην υπάρχουν έγγραφα πάνω στο γραφείο χωρίς την παρουσία υπαλλήλου και αντίστοιχα να μην μένει ανοικτή η οθόνη.
- Αφαίρεση εξοπλισμού

Στόχος: Η διασφάλιση της σωστής και ασφαλούς λειτουργίας των πληροφοριακών συστημάτων.

Θα πρέπει να καταγράφονται αρμοδιότητες και διαδικασίες για τη διαχείριση και τη λειτουργία όλων των πληροφοριακών υποδομών. Θα πρέπει να επιβάλλεται διαχωρισμός καθηκόντων όπου αυτό απαιτείται για να ελαττώσει τον κίνδυνο αμέλειας ή εκούσιας εκμετάλλευσης των συστημάτων. (π.χ. άλλος θα πρέπει να εκδίδει τις επιταγές και άλλος να τις υπογράφει).

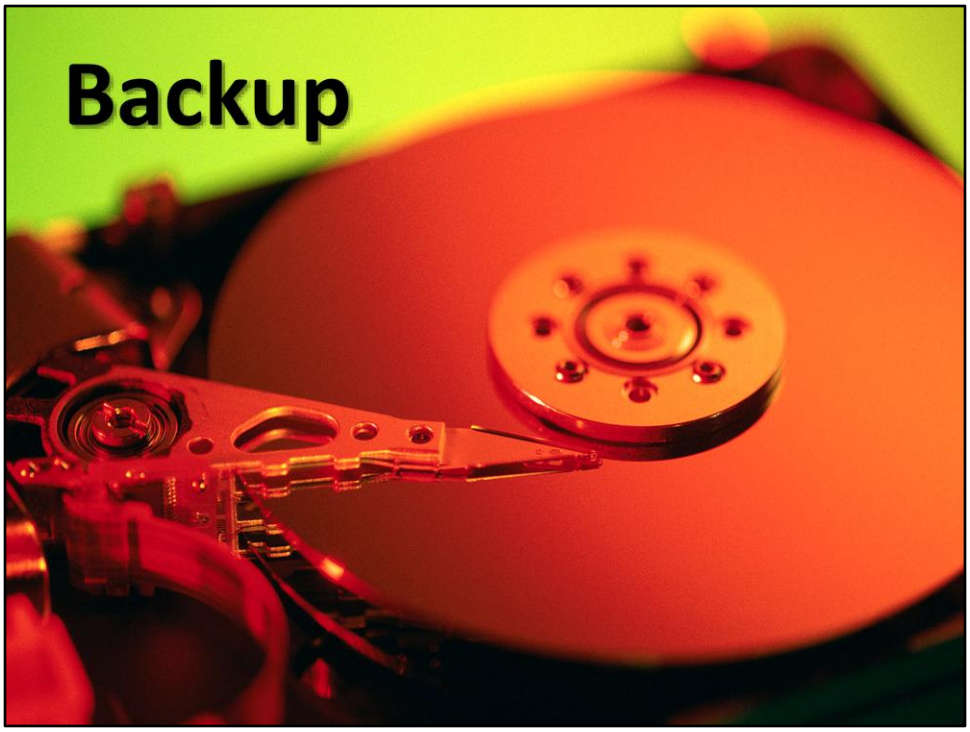


Προστασία από κακόβουλο και κινητό κώδικα

Στόχος: Η προστασία της ακεραιότητας του λογισμικού εφαρμογών και των αντίστοιχων πληροφοριών.

Απαιτούνται μέτρα προστασίας για τον εντοπισμό και την προστασία από την εισαγωγή κακόβουλου κώδικα και μη εξουσιοδοτημένου κινητού κώδικα.

Λογισμικό και υποδομές που επεξεργάζονται πληροφορίες είναι ευάλωτες στην εισαγωγή κακόβουλου κώδικα, όπως ιομορφικού λογισμικού, σκουληκιών, δούρειων ίππων, κλπ. Οι χρήστες θα πρέπει να γνωρίζουν τους κινδύνους του κακόβουλου κώδικα. Η διοίκηση θα πρέπει να εισάγει μηχανισμούς προστασίας όπου απαιτείται για την πρόληψη, εντοπισμό και διαγραφή του κακόβουλου κώδικα και για τον έλεγχο του κινητού κώδικα.



Στόχος: η διασφάλιση της ακεραιότητας και διαθεσιμότητας των πληροφοριών και των αντίστοιχων συστημάτων

Θα πρέπει να καταγράφονται διαδικασίες για την υλοποίηση των πολιτικών ασφάλειας και τον έλεγχο ορθής λήψης αντιγράφων. Θα πρέπει ανά τακτά χρονικά διαστήματα να ελέγχεται ότι τα αντίγραφα λαμβάνονται σωστά, με προσπάθειες επαναφοράς των δεδομένων.

Στόχος: Η προστασία των πληροφοριών στα δίκτυα και στην αντίστοιχη δικτυακή υποδομή.

Η ασφαλής διαχείριση των δικτύων, τα οποία μπορεί να επεκτείνουν τα επιχειρησιακά όρια πέρα από τη φυσική περίμετρο του οργανισμού, είναι ιδιαίτερης σημασίας καθώς επηρεάζει τη ροή των δεδομένων και μπορεί να έχει νομικές επιπτώσεις όσον αφορά την παρακολούθηση και την προστασία τους.

Επιπλέον μέτρα μπορεί να απαιτούνται για την προστασία ευαίσθητων πληροφοριών που διακινούνται μέσα από δημόσια δίκτυα.

Στόχος: Η πρόληψη μη εξουσιοδοτημένης αποκάλυψης, αλλαγής, ή καταστροφής των αγαθών και διακοπής των επιχειρησιακών λειτουργιών του οργανισμού.
Τα αποσπώμενα μέσα πρέπει να ελέγχονται και να προστατεύονται φυσικά.

Πρέπει να υπάρχουν κατάλληλες λειτουργικές διαδικασίες για την προστασία εγγράφων, μέσων (π.χ. κασέτες, δίσκοι, usb disks κλπ.), δεδομένων εισόδου/εξόδου και τεκμηρίωσης συστημάτων από μη εξουσιοδοτημένη αποκάλυψη, μετατροπή, διαγραφή ή καταστροφή

Συνολική διαχείριση αφαιρούμενων συσκευών. (π.χ. «διαφημιστικό» usb το οποίο περιέχει κακόβουλο λογισμικό που τρέχει μόλις συνδεθεί σε υπολογιστή και μπορεί να μολύνει το εταιρικό δίκτυο ή να αποσπάσει εμπιστευτικές πληροφορίες. Επίσης χαμένα ή κλεμμένα laptops ή usb sticks)
Διαδικασίες για ασφαλή καταστροφή τους (π.χ. σύμφωνα με Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)

Στόχος: Εντοπισμός μη εξουσιοδοτημένων ενεργειών

Τα συστήματα θα πρέπει να παρακολουθούνται ώστε να καταγράφονται τα περιστατικά ασφάλειας.
Θα πρέπει να χρησιμοποιούνται αρχεία καταγραφής (audit logs) για να διασφαλίζεται ο έγκυρος εντοπισμός προβλημάτων.
Ένας οργανισμός θα πρέπει επίσης να συμμορφώνεται με αντίστοιχες νομικές και κανονιστικές απαιτήσεις όσον αφορά την παρακολούθηση και καταγραφή συμβάντων.
Τα συστήματα παρακολούθησης θα πρέπει να χρησιμοποιούνται και για να ελέγχουν την αποτελεσματικότητα των μηχανισμών ασφάλειας που έχουν υιοθετηθεί και για να επιβεβαιώνουν τη σωστή χρήση της πολιτικής ασφάλειας και των μοντέλων ελέγχου προσπέλασης.

Επιπλέον, τα αρχεία καταγραφής θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη προσπέλαση, διαγραφή ή τροποποίηση, καθότι είναι ιδιαίτερα κρίσιμα ως προς τη διερεύνηση συμβάντων. («logs don’t lie»)

Επιχειρησιακές απαιτήσεις ελέγχου πρόσβασης
- Πολιτική ελέγχου πρόσβασης

Διαχείριση πρόσβασης χρηστών
- Εγγραφή χρηστών, Διαχείριση προνομίων, Διαχείριση συνθηματικών, Έλεγχος δικαιωμάτων πρόσβασης χρηστών

Ευθύνες χρηστών
- Χρήση συνθηματικού, Επίβλεψη εξοπλισμού χρηστών

Έλεγχος δικτυακής πρόσβασης
- Πολιτική χρήσης δικτυακών πόρων, Υποχρεωτική δρομολόγηση, Αυθεντικοποίηση χρηστών από εξωτερικές συνδέσεις
- Αυθεντικοποίηση κόμβου, Προστασία θύρας απομακρυσμένης διάγνωσης, Διαχωρισμός δικτύων
- Έλεγχος συνδεσιμότητας δικτύου, Έλεγχος δρομολόγησης δικτύου, Ασφάλεια δικτυακών υπηρεσιών

Έλεγχος πρόσβασης ΛΣ
- Αυτόματη αναγνώριση τερματικού, Διαδικασία σύνδεσης τερματικού, Αναγνώριση και αυθεντικοποίηση χρηστών
- Σύστημα διαχείρισης συνθηματικών, Χρήση πόρων συστήματος, Time-out τερματικού, Περιορισμός χρόνου σύνδεσης

Έλεγχος πρόσβασης εφαρμογών
- Περιορισμός πρόσβασης στην πληροφορία
- Απομόνωση ευαίσθητων συστημάτων

Παρακολούθηση πρόσβασης και χρήσης
- Καταγραφή συμβάντων, Παρακολούθηση χρήσης συστήματος, Συγχρονισμός ρολογιών

Κινητό υπολογίζειν και τηλεργασία
- Κινητό υπολογίζειν, Τηλεργασία

Απαιτήσεις ασφάλειας συστημάτων
- Ανάλυση και προδιαγραφές

Ασφάλεια σε εφαρμογές
- Επικύρωση δεδομένων εισόδου, Έλεγχος εσωτερικής επεξεργασίας, Αυθεντικοποίηση μηνυμάτων, Επικύρωση δεδομένων εξόδου

Ασφάλεια διαδικασιών ανάπτυξης και υποστήριξης
- Διαδικασίες ελέγχου αλλαγών, Τεχνικός έλεγχος αλλαγών ΛΣ, Περιορισμοί αλλαγών λογισμικού
- Κανάλια συγκαλυμμένης μετάδοσης και δούρειοι ίπποι, Ανάπτυξη λογισμικού με outsourcing

Κρυπτογραφικά μέτρα προστασίας
- Πολιτική χρήσης, Κρυπτογράφηση, Ψηφιακές υπογραφές, Υπηρεσίες μη αποποίησης, Διαχείριση κλειδιών

Ασφάλεια αρχείων συστήματος
- Έλεγχος λειτουργικού λογισμικού, Προστασία δεδομένων ελέγχου συστήματος, Έλεγχος πρόσβασης σε βιβλιοθήκες συστήματος

Στόχος: Να διασφαλίσουμε ότι διαχειριζόμαστε περιστατικά και αδυναμίες ασφάλειας των πληροφοριακών και τηλεπικοινωνιακών συστημάτων με τέτοιο τρόπο που να επιτρέπει έγκαιρη αντιμετώπισή τους.
Πρέπει να υπάρχουν επίσημες αναφορές περιστατικών και διαδικασίες αντιμετώπισης. Υπάλληλοι, συνεργάτες και τρίτοι φορείς οφείλουν να γνωρίζουν τις διαδικασίες αναφορών για τα διάφορα περιστατικά και τις αδυναμίες που μπορεί να έχουν επιπτώσεις στην ασφάλεια των αγαθών. Οφείλουν να αναφέρουν κάθε περιστατικό ασφάλειας ή αδυναμία το συντομότερο δυνατό.

Καταγραφή αντίστοιχων ρόλων, αρμοδιοτήτων και διαδικασιών

Στόχος: Η συστηματική και αποτελεσματική διαχείριση των περιστατικών ασφάλειας

Θα πρέπει να καταγράφονται αρμοδιότητες και διαδικασίες για τη διαχείριση περιστατικών ασφάλειας και αδυναμιών με αποτελεσματικότητα, μόλις αυτά αναφερθούν. Θα πρέπει επίσης να υπάρχει μια διαδικασία διαρκούς βελτίωσης όσον αφορά την ανταπόκριση, παρακολούθηση, αξιολόγηση και γενικά διαχείριση των περιστατικών ασφάλειας.

Όπου απαιτούνται στοιχεία, αυτά θα πρέπει να συλλέγονται σύμφωνα με τις εκάστοτε νομικές απαιτήσεις. Για το σκοπό αυτό υπάρχουν συγκεκριμένες τεχνικές και εργαλεία λήψης ψηφιακών πειστηρίων (digital forensics)

Στόχος: Η αντιμετώπιση των επιπτώσεων και των διακοπών στις επιχειρησιακές λειτουργίες και η προστασία κρίσιμων επιχειρησιακών διαδικασιών από μεγάλες αστοχίες πληροφοριακών συστημάτων ή καταστροφές, ώστε να διασφαλιστεί η έγκαιρη επαναλειτουργία τους.

Μια διαδικασία διαχείρισης της επιχειρησιακής συνέχεια πρέπει να υλοποιηθεί για να περιορίσει τις επιπτώσεις στον οργανισμό και να διασφαλίσει την επαναφορά των αγαθών σε ένα αποδεκτό επίπεδο, μετά από π.χ. φυσικές καταστροφές, ατυχήματα, αστοχία εξοπλισμού και εκούσιες ενέργειες. Για το σκοπό αυτό πρέπει να χρησιμοποιούνται αποτρεπτικά μέτρα καθώς και μέτρα ανάκτησης λειτουργίας. Η διαδικασία αυτή θα πρέπει να εντοπίζει τις κρίσιμες επιχειρησιακές διαδικασίες και να ενσωματώνει στη διαχείριση της ασφάλειας πληροφοριών τις απαιτήσεις επιχειρησιακή συνέχειας όσον αφορά τις διάφορες λειτουργίες, τη στελέχωση, το υλικό, τα μέσα μετακινήσεων και τις υποδομές.

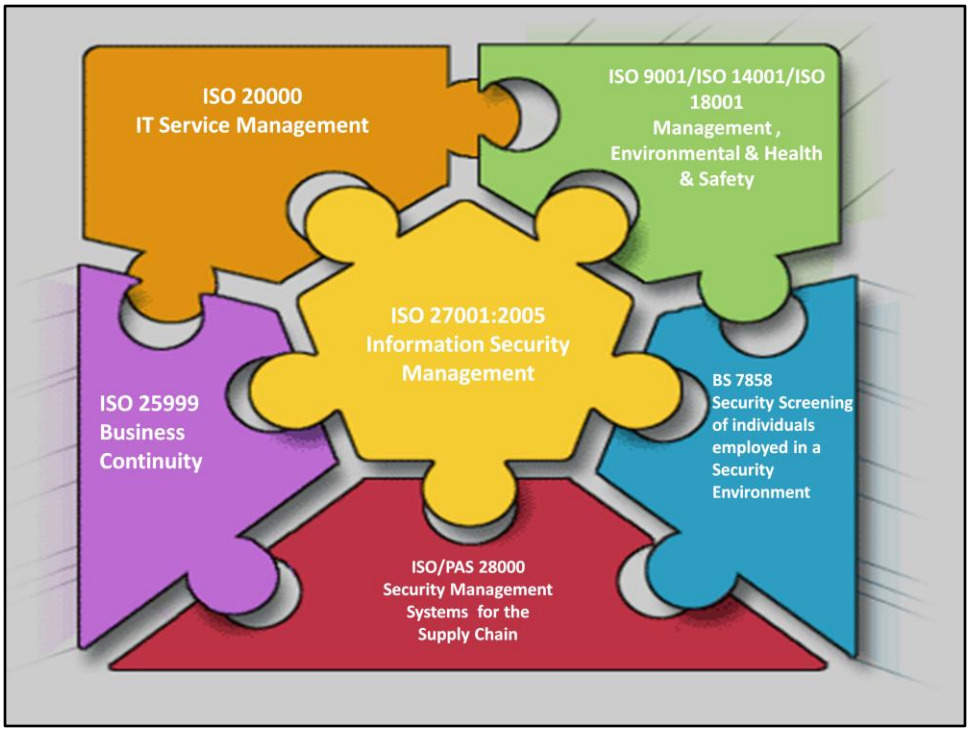
Οι επιπτώσεις των καταστροφών, των παραβιάσεων ασφάλειας, της απώλειας υπηρεσιών και της διαθεσιμότητας θα πρέπει να είναι αντικείμενο της Ανάλυσης Επιχειρησιακών Επιπτώσεων (Business Impact Analysis). Πλάνα επιχειρησιακής συνέχεια θα πρέπει να αναπτυχθούν και να υλοποιηθούν για να διασφαλιστεί η έγκαιρη επαναλειτουργία κρίσιμων υπηρεσιών. Η ασφάλεια πληροφοριών πρέπει να αποτελεί αναπόσπαστο κομμάτι της συνολικής διαδικασίας επιχειρησιακής συνέχειας.
Η διαχείριση της επιχειρησιακής συνέχειας θα πρέπει να περιλαμβάνει ελεγκτικούς μηχανισμούς για να εντοπιστούν και να μειωθούν οι κίνδυνοι, να περιοριστούν οι συνέπειες από περιστατικά ασφάλειας για να διασφαλίσει ότι οι πληροφορίες που απαιτούνται για τις επιχειρησιακές διαδικασίες είναι άμεσα διαθέσιμες.

Διαδικασία υλοποίησης:
•Ανάλυση επιπτώσεων και συνέχιση λειτουργίας
•Διαμόρφωση σχεδίων επιχειρησιακής συνέχειας
•Πλαίσιο σχεδίου επιχειρησιακής συνέχειας
•Δοκιμές, συντήρηση και επανεκτίμηση σχεδίων

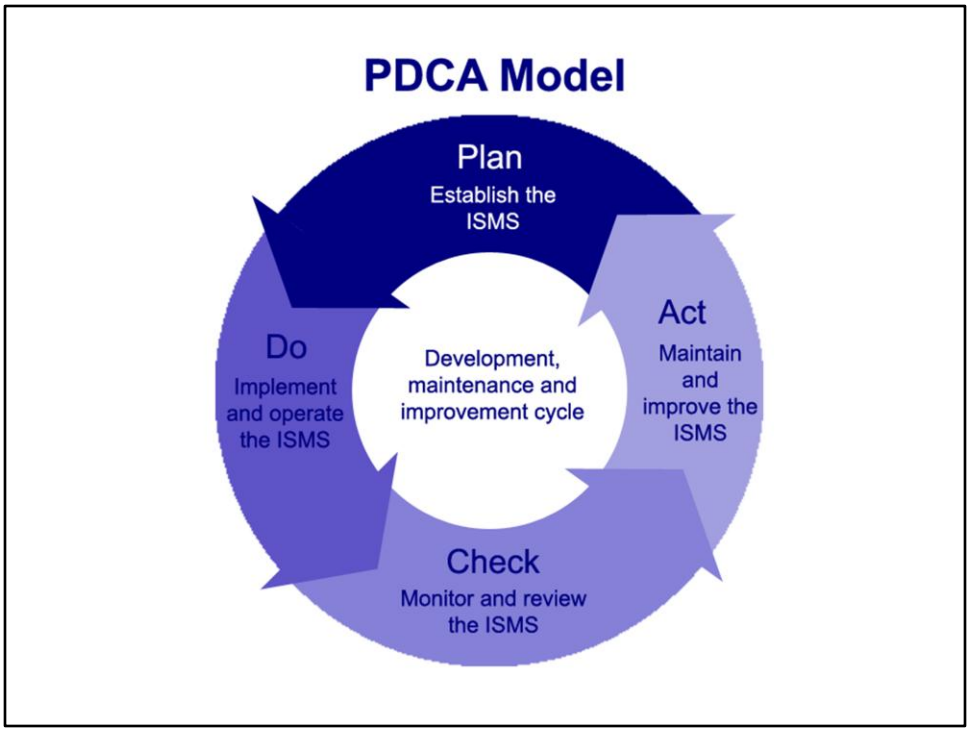
Με νομικές υποχρεώσεις
- Αναγνώριση σχετικής νομοθεσίας
- Δικαιώματα πνευματικής ιδιοκτησίας
- Προστασία οργανωσιακών αρχείων
- Προστασία προσωπικών πληροφοριών
- Πρόληψη κατάχρησης συστημάτων επεξεργασίας πληροφοριών
- Κανονισμοί κρυπτογραφίας
- Συλλογή πειστηρίων

Επανεκτιμήσεις πολιτικής και τεχνική συμμόρφωση
- Συμμόρφωση με την πολιτική
- Έλεγχος τεχνικής συμμόρφωσης

Ελεγκτική συστημάτων
- Μέτρα ελεγκτικής
- Προστασία εργαλείων ελεγκτικής



Κοινά σημεία με άλλες οικογένειες προτύπων ISO.



Υλοποίηση: Μοντέλο PDCA model

Εκκίνηση του έργου
Διασφάλιση της συναίνεσης της διοίκηση
Επιλογή και εκπαίδευση μελών της ομάδας έργου]

Ορισμός του ΣΔΑΠ
Ορισμός των στόχων και του εύρους του πλαισίου διαχείρισης ασφάλειας πληροφοριών

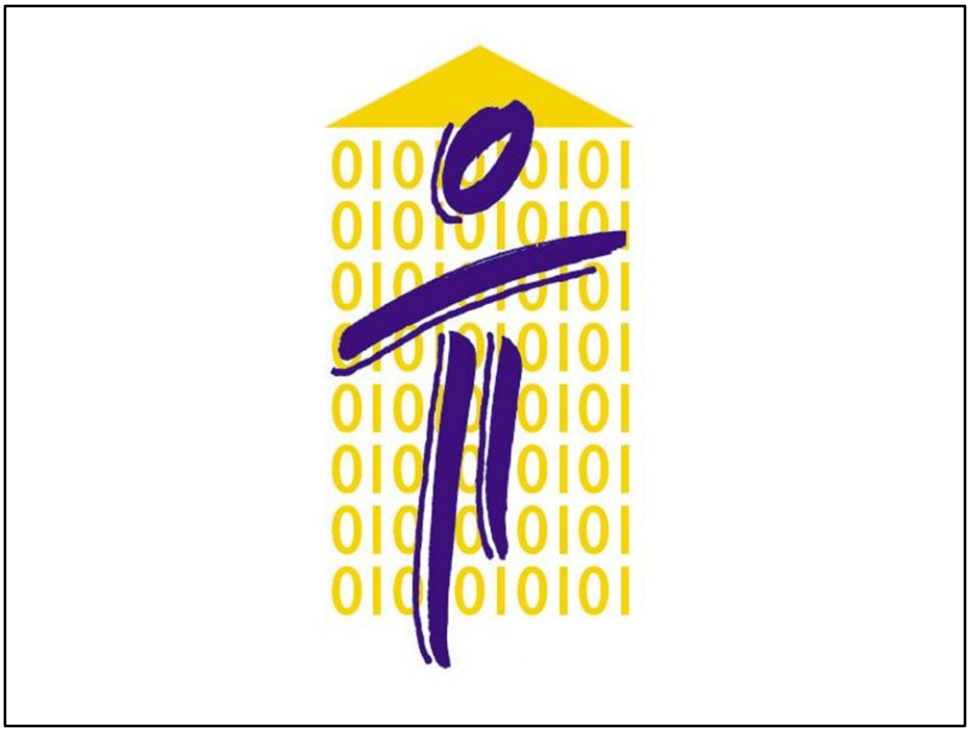
Αποτίμηση Επικινδυνότητας
Δημιουργία καταλόγου προς προστασία αγαθών (Inventory) και αποτίμησή τους.
Εντοπισμός και αποτίμηση απειλών και ευπαθειών
Αποτίμηση κινδύνων που εντοπίζονται σε όλες τις περιοχές ελέγχου.
Υπολογισμός τιμών των κινδύνων αυτών

Αντιμετώπιση Κινδύνων
Επιλογή ενός συστήματος ελεγκτικών μηχανισμών και στόχων που είναι κατάλληλοι για τη διαχείριση και την αντιμετώπιση των κινδύνων με λογικό κόστος.
Υπολογισμός του κατά πόσο η επιλογή και η υλοποίηση των σωστών μηχανισμών μπορεί να ελαττώσει τους κινδύνους του οργανισμού σε ένα αποδεκτό επίπεδο.
Προετοιμασία μίας δήλωσης εφαρμοσιμότητας (Statement of Applicability). Το κείμενο αυτό παρουσιάζει τους στόχους των ελεγκτικών μηχανισμών που επιλέχθηκαν και τους συνδέει με τα αποτελέσματα της αποτίμησης κινδύνων.
Έλεγχος επιπέδου συμμόρφωσης με το ISO 27001.

Εκπαίδευση και ευαισθητοποίηση
Τα στελέχη και οι υπάλληλοι μπορεί να είναι ο πιο αδύναμος κρίκος για την ασφάλεια πληροφοριών σε έναν οργανισμό.

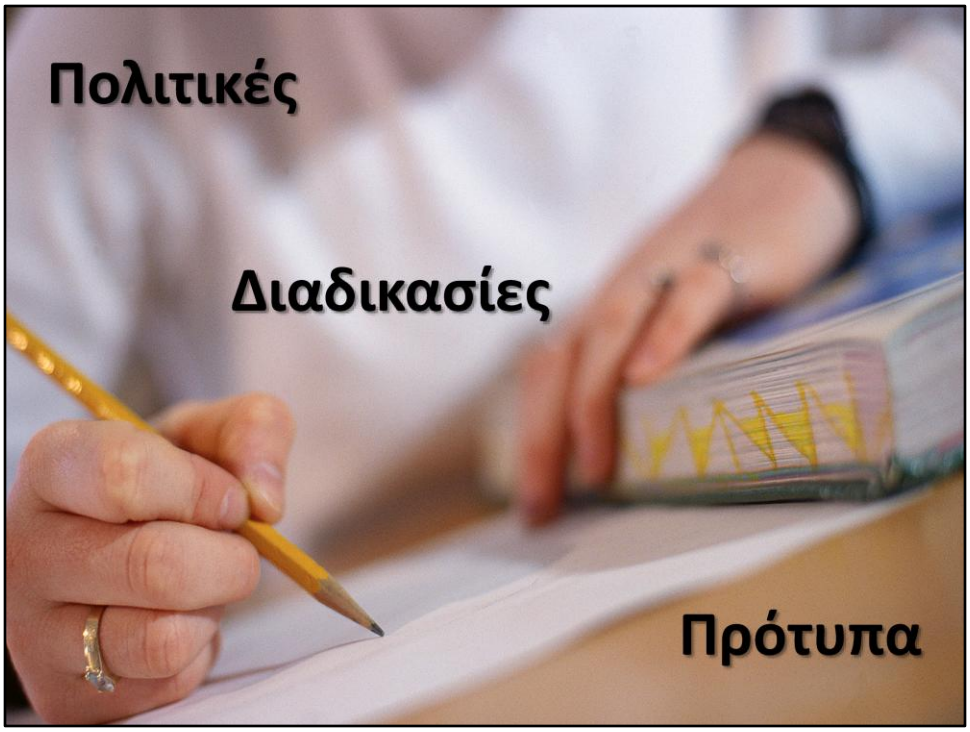
Προετοιμασία για Έλεγχο
Εσωτερικός έλεγχος

Εξωτερικός Έλεγχος (letter of opinion)
Πιστοποίηση



Γιατί να υλοποιήσουμε μια πολιτική ασφάλειας: Μεταξύ άλλων υποχρεώνουν οι σχετικοί νόμοι-κανονιστικές διατάξεις. Π.χ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα: «Κάθε οργανισμός που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα οφείλει να τηρεί σχέδιο ασφάλειας»

«Το **Σχέδιο Ασφάλειας (Security Plan)** είναι το έγγραφο στο οποίο περιγράφεται η πολιτική ενός οργανισμού για την κάλυψη των βασικών απαιτήσεων ασφάλειας, καθώς επίσης και τα κύρια τεχνικά, διοικητικά και οργανωτικά μέτρα ασφάλειας που εφαρμόζονται ή/και πρόκειται να εφαρμοστούν, συμπεριλαμβανομένου του πλάνου πραγματοποίησης και επισκόπησης/αναθεώρησής τους.»



Οι οδηγίες και τα μέτρα προστασίας πρέπει να καλύπτουν το σύνολο των αγαθών του ΠΣ και όλες τις λειτουργίες του (πληρότητα).
Πρέπει να λαμβάνονται υπόψη οι τρέχουσες τεχνολογικές εξελίξεις (επικαιρότητα).
Με κάποιες τροποποιήσεις ή προσθήκες να μπορεί η Πολιτική να καλύπτει μικρές αλλαγές ή επεκτάσεις στα ΠΣ (γενικευσιμότητα).
Πολιτική Ασφάλειας απευθύνεται στο σύνολο των μελών του οργανισμού και θα πρέπει να είναι εύκολα κατανοητή από όλους (σαφήνεια και ευκολία κατανόησης).
Η περιγραφή των μέτρων ασφάλειας δε θα πρέπει να δεσμεύει τον οργανισμό σε συγκεκριμένα προϊόντα και τεχνολογίες (τεχνολογική ανεξαρτησία).
Οι απαιτήσεις ασφάλειας πρέπει να καλύπτουν τις ανάγκες του συγκεκριμένου οργανισμού (καταλληλότητα).
Τα μέτρα προστασίας θα πρέπει να μπορούν να εφαρμοστούν χωρίς να δυσχεραίνουν δυσανάλογα τις δραστηριότητες των χρηστών του ΠΣ (εφαρμοσιμότητα).

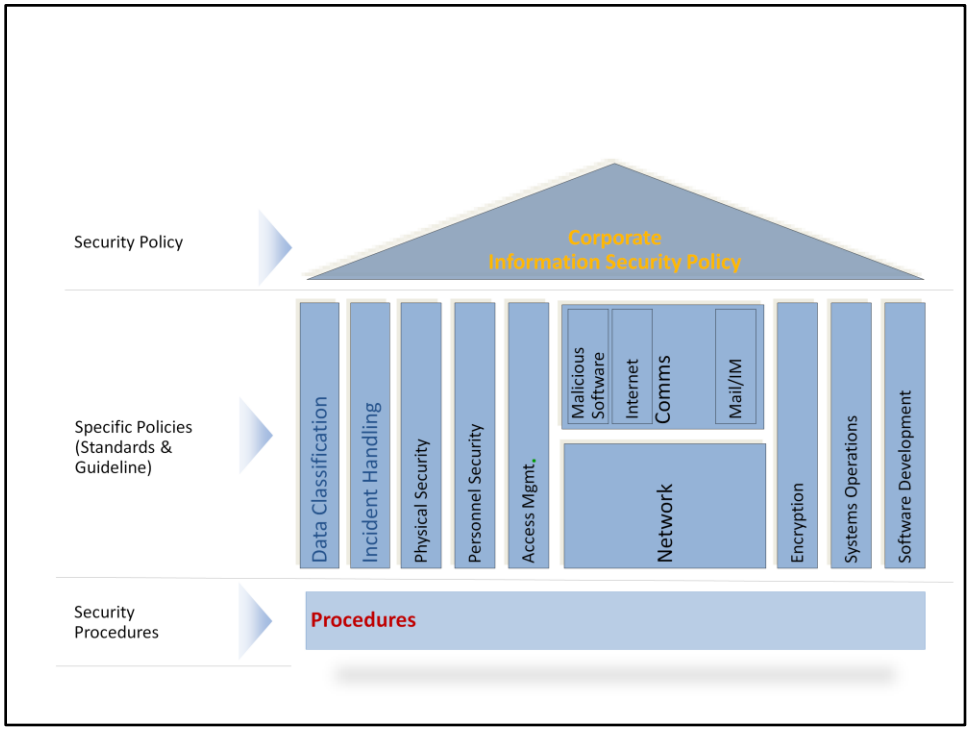
Τα πρότυπα (*Standards)* ορίζουν υποχρεωτικές απαιτήσεις για την ομογενοποιημένη χρήση του hardware, του λογισμικού, της τεχνολογίας και των μηχανισμών ασφάλειας. Παρέχουν οδηγίες με τις οποίες τεχνολογίες και διαδικασίες υλοποιούνται σε έναν οργανισμό. Αποτελούν κείμενα που ορίζουν βήματα ή μεθόδους για την υλοποίηση των στόχων και της συνολικής κατεύθυνσης της πολιτικής ασφάλειας.

Στο επόμενο επίπεδο βρίσκονται τα baselines τα οποία ορίζουν ένα ελάχιστο επίπεδο ασφάλειας το οποίο πρέπει να καλύπτει κάθε σύστημα στον οργανισμό.

Τα *guidelines* αποτελούν συστάσεις υλοποίησης των standards και baselines και αποτελούν οδηγούς υλοποίησης για υπεύθυνους ασφάλειας και τελικούς χρήστες.

Η διαδικασία (*procedure)* είναι μια αναλυτική περιγραφή των συγκεκριμένων βημάτων που απαιτούνται για την υλοποίηση ενός συγκεκριμένου μηχανισμού ασφάλειας ή λύσης. Συνήθως περιγράφει συνοίκά την υλοποίηση ενός προϊόντος (π.χ. Firewall) ή πώς θα ενημερώνεται το antivirus.

Π.χ. η πολιτική ορίζει ότι η απομακρυσμένη πρόσβαση στα συστήματα πρέπει να υλοποιείται με εμπιστευτικότητα. Ένα baseline ορίζει ότι τα δεδομένα που κινούνται στο δίκτυο πρέπει να είναι κρυπτογραφημένα. Το guideline λέει ότι η απομακρυσμένη πρόσβαση πρέπει να υλοποιηθεί με VPN και μια διαδικασία ορίζει επακριβώς την τεχνολογία που θα χρησιμοποιηθεί (π.χ. Cisco) και τα βήματα για τις ρυθμίσεις. Το αντίστοιχο πρότυπο αναφέρει ότι τα laptop μόνο επιτρέπεται να φέρουν το σύστημα απομακρυσμένης πρόσβασης το οποίο πρέπει να είναι κοινό.



Συνήθως υλοποιούνται 2 ή 3 επίπεδα πολιτικών και ένα επίπεδο διαδικασιών.
Στην κορυφή υπάρχει μία εταιρική πολιτική ασφάλειας, γενικού περιεχομένου, μικρή σε μέγεθος, που να μπορεί να γίνει κατανοητή από οποιονδήποτε.
Σε δεύτερο επίπεδο καταγράφονται τεχνικές πολιτικές ασφάλειας, που απευθύνονται σε συγκεκριμένα τμήματα και είναι πιο συγκεκριμένες.

Μια Πολιτική Ασφάλειας ΠΣ επιτυγχάνει καλύτερα τους στόχους της όταν:

- υποστηρίζει τους επιχειρηματικούς στόχους του οργανισμού.
- η ανώτερη διοίκηση του οργανισμού υποστηρίζει και συμμετέχει ενεργά στην εφαρμογή της.
- είναι κατάλληλη για το συγκεκριμένο περιβάλλον όπου εφαρμόζεται (οργανωσιακή κουλτούρα).
- οι χρήστες εκπαιδεύονται και ενημερώνονται κατάλληλα.

…και όταν

- υπάρχουν διαδικασίες αξιολόγησης της αποτελεσματικότητάς της, ώστε να αναθεωρείται κατάλληλα.
- εφαρμόζεται σταδιακά, ανάλογα με το βαθμό της αλλαγής που επιφέρει η εφαρμογή της Πολιτικής στις δραστηριότητες των χρηστών.
- έχουν εύκολη και άμεση πρόσβαση σε αυτήν όλοι οι χρήστες του ΠΣ.


PCi
Security
Standards Council
™

Ιστορία του PCI DSS

- **Το Σεπτέμβριο του 2006 το PCI Security Standards Council δημιουργείται από:**
  - Την American Express, την Discover Financial Services, την JCB, τη MasterCard Worldwide, και την Visa International
  - Χρίζεται υπεύθυνο για τις τις λειτουργίες PCI DSS και τις λειτουργίες για δικτυακούς ελέγχους
  - Χρίζεται υπεύθυνο για το σώμα των Qualified Security Assessor (QSA) και των Approved Scanning Vendor (ASV)
    - Πιστοποιεί εταιρείες για να πραγματοποιούν ελέγχους ασφάλειας πληροφορικής (Information Security Audits)
    - Πιστοποιεί εταιρείες για να πραγματοποιούν δικτυακούς ελέγχους ασφαλείας
  - Απελευθερώνει το PCI DSS v1.2 δημιουργώντας νέες διαδικασίες συμβατότητας.

PCI Standards

- **PCI Data Security Standard (DSS)**

  Αφορά όλες τις οντότητες που αποθηκεύουν, επεξεργάζονται ή/και μεταδίδουν δεδομένα κατόχων πιστωτικών καρτών (cardholder data). Καλύπτει τεχνικά και οργανωτικά θέματα. Όλοι οι έμποροι που δέχονται ή επεξεργάζονται πιστωτικές κάρτες πρέπει να καλύπτουν τις απαιτήσεις του PCI DSS.
- **PIN Transaction Security (PTS) Requirements**

  Το PCI PTS (πρώην PCI PED) είναι ένα σύνολο από απαιτήσεις ασφάλειας που αφορούν τα χαρακτηριστικά και τη διαχείριση των συσκευών που χρησιμοποιούνται για την προστασία των PIN και την επεξεργασία των συναλλαγών. Οι κατασκευαστές οφείλουν να ακολουθούν τις απαιτήσεις στο σχεδιασμό, την κατασκευή και τη μεταφορά της συσκευής. Χρηματοπιστωτικά ιδρύματα, έμποροι και πάροχοι υπηρεσιών οφείλουν να χρησιμοποιούν μόνο συσκευές που έχουν ελεγχθεί και εγκριθεί από το PCI

  www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php
- **Payment Application Data Security Standard (PA-DSS)**

  Το PA-DSS αφορά όσους αναπτύσσουν λογισμικό για εφαρμογές πληρωμών που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα πιστωτικών καρτών. Οι περισσότερες εταιρίες πιστωτικών καρτών ενθαρρύνουν τους εμπόρους να χρησιμοποιούν εφαρμογές που έχουν ελεγχθεί και πιστοποιηθεί από το PCI

  www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

Γιατί PCI DSS;

- **ΟΛΟΙ** οι οργανισμοί που κάνουν χρήση πιστωτικών καρτών για ηλεκτρονικές συναλλαγές πρέπει να είναι συμβατοί με το πρότυπο **PCI DSS**.

- Το 2005 μόνο η VISA συνέλεξε το ποσό των 3.4 εκατομμυρίων δολαρίων από πρόστιμα μη συμβατότητας με το πρότυπο PCI DSS,
  ενώ το 2006 4.6 εκατομμύρια δολάρια .

Απαιτήσεις του PCI DSS

(Α) Δημιουργία και συντήρηση ασφαλούς δικτύου

- Εγκατάσταση και συντήρηση firewall για την προστασία των δεδομένων των πιστωτικών καρτών.
- Βεβαίωση μη χρήσης default passwords και άλλων default παραμέτρων ασφάλειας.

(Β) Προστασία των δεδομένων των πιστωτικών καρτών

- Προστασία των αποθηκευμένων δεδομένων στα διάφορα ηλεκτρονικά μέσα.
- Προστασία των δεδομένων των πιστωτικών καρτών κατά την μετάδοση τους από και προς δημόσια και ανοικτά δίκτυα.

(Γ) Διατήρηση προγράμματος επικινδυνότητας

- Χρήση αντιβιοτικού που ενημερώνεται συχνά.
- Ανάπτυξη και χρήση ασφαλών εφαρμογών.

Απαιτήσεις του PCI DSS

(Δ) Ισχυρά μέτρα ασφάλειας πρόσβασης

- Περιορισμός των δεδομένων των πιστωτικών καρτών μόνο σε άτομα που απαιτείται (need to know)
- Χρήση μοναδικού αναγνωριστικού ανά άτομο με πρόσβαση μέσω υπολογιστή στα δεδομένα των πιστωτικών καρτών (unique ID assignment).
- Έλεγχος στη φυσική πρόσβαση των δεδομένων των πιστωτικών καρτών.

(Ε) Παρακολούθηση και έλεγχος δικτυακής υποδομής

- Παρακολούθηση όλων δικτυακών προσβάσεων στα δεδομένα των δικαιούχων των πιστωτικών καρτών
- Συχνά τεστ σε επίπεδο ασφάλειας των συστημάτων που διαχειρίζονται τα δεδομένα.

(Ζ) Διατήρηση πολιτικών ασφαλείας

- Διατήρηση πολιτικών ασφάλειας και συνεχή παρακολούθηση των θεμάτων που αφορούν την ασφάλεια πληροφοριών.

Ποιους αφορά το PCI DSS;

- **Όλους τους συνεργάτες της Visa:**

- **Εκδότριες τράπεζες (Issuer Banks):**
  - ✓ Οι τράπεζες που εκδίδουν κάρτες Visa στους πελάτες τους.

- **Αποδέκτριες τράπεζες (Acquirer Banks ή Merchant Banks):**
  - ✓ Οι τράπεζες που συμβάλλονται με εμπόρους, ώστε οι τελευταίοι να μπορούν να αποδέχονται πληρωμές με κάρτες Visa.

- **Έμποροι (Merchants):**
  - ✓ Οι επιχειρήσεις που αποδέχονται κάρτες Visa.

Ποιους αφορά το PCI DSS;

- Οι δημιουργοί του προτύπου χωρίζουν τους υπευθύνους σε δυο βασικές κατηγορίες:
  1. Τους παρόχους υπηρεσιών (Service Providers)
  2. Τους εμπόρους (Merchants)

- **Ποιος είναι έμπορος για το PCI DSS;**
  - Οι έμποροι ορίζονται ως αυτοί που τυπικά δέχονται απευθείας την πληρωμή από τους πελάτες.

- **Ποιος είναι πάροχος υπηρεσιών για το PCI DSS: :**
  - Οι πάροχοι υπηρεσιών ορίζονται ως αυτοί που τυπικά επεξεργάζονται τις ηλεκτρονικές συναλλαγές για λογαριασμό των εμπόρων.

Κατηγορίες εμπόρων

	Προαπαιτούμενα	Απαιτήσεις	Πραγματοποιείται από:
Επίπεδο 1	1. Πραγματοποιούν 6,000,000 συναλλαγές το χρόνο ή 2. Είχαν περιστατικά υπονόμευσης δεδομένων πιστωτικής κάρτας τον προηγούμενο χρόνο ή 3. Έχει χαρακτηριστεί ως έμπορος επιπέδου 1 από άλλη εταιρία πιστωτικών καρτών.	1. Ετήσιο On-Site Audit 2. Τρίμηνη ανάλυση επικινδυνότητας δικτύου	1. QSA 2. Qualified Independent Scan Vendor
Επίπεδο 2	Πραγματοποιούν από 1,000,000 έως 6,000,000 συναλλαγές το χρόνο.	1. Ετήσιο self-assessment 2. Τρίμηνη ανάλυση επικινδυνότητας δικτύου	1. Merchant 2. Qualified Independent Scan Vendor (ASV)
Επίπεδο 3	Πραγματοποιούν από 20,000 έως 1,000,000 **διαδικτυακές** συναλλαγές το χρόνο.	1. Ετήσιο self-assessment 2. Τρίμηνη ανάλυση επικινδυνότητας δικτύου	1. Merchant 2. Qualified Independent Scan Vendor (ASV)
Επίπεδο 4	Που πραγματοποιούν λιγότερες από 20,000 το χρόνο διαδικτυακές συναλλαγές (μέσο Web).	1. **Συνιστάται** Ετήσιο self-assessment 2. **Συνιστάται** τρίμηνη ανάλυση επικινδυνότητας δικτύου.	1. Merchant 2. Qualified Independent Scan Vendor (ASV)

Κατηγορίες για τους παρόχους υπηρεσιών

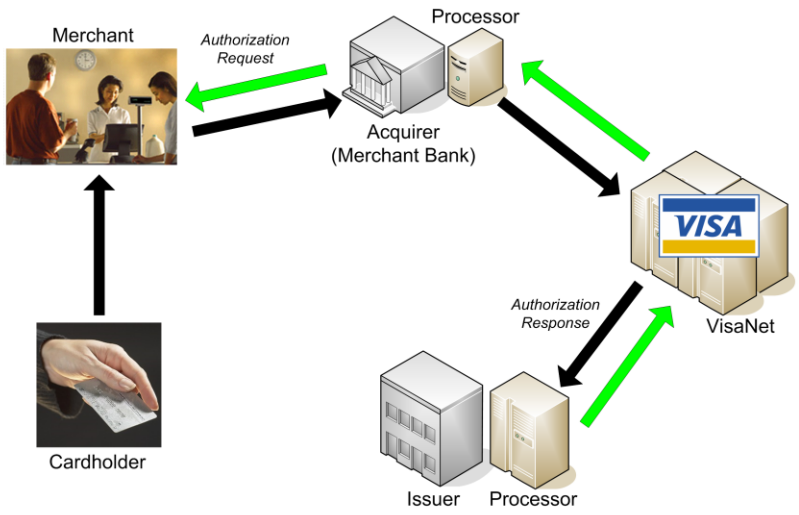
	Προαπαιτούμενα	Απαιτήσεις	Πραγματοποιείται από:
Επίπεδο 1	1. Όλοι οι VisaNet processors 2. Payment Gateways 3. Internet Payment Service Providers (ανεξάρτητα από το μέγεθος των συναλλαγών)	1. Ετήσιο On-Site Audit 2. Τρίμηνη ανάλυση επικινδυνότητας δικτύου	1. QSA 2. Qualified Independent Scan Vendor
Επίπεδο 2	Όλοι οι παροχείς υπηρεσιών που δεν είναι Επίπεδο 1 και αποθηκεύουν , επεξεργάζονται περισσότερες από**1,000,000 συναλλαγές το χρόνο.** .	1. Ετήσιο On-Site Audit 2. Τρίμηνη ανάλυση επικινδυνότητας δικτύου	1. QSA 2. Qualified Independent Scan Vendor
Επίπεδο 3	Όλοι οι παροχείς υπηρεσιών που δεν είναι Επίπεδο 1 και αποθηκεύουν , επεξεργάζονται λιγότερο από**1,000,000 συναλλαγές το χρόνο.**	1. Ετήσιο Self-Assessment 2. Τρίμηνη ανάλυση επικινδυνότητας δικτύου	1. Service Provider 2. Qualified Independent Scan Vendor

Πρόστιμα PCI DSS

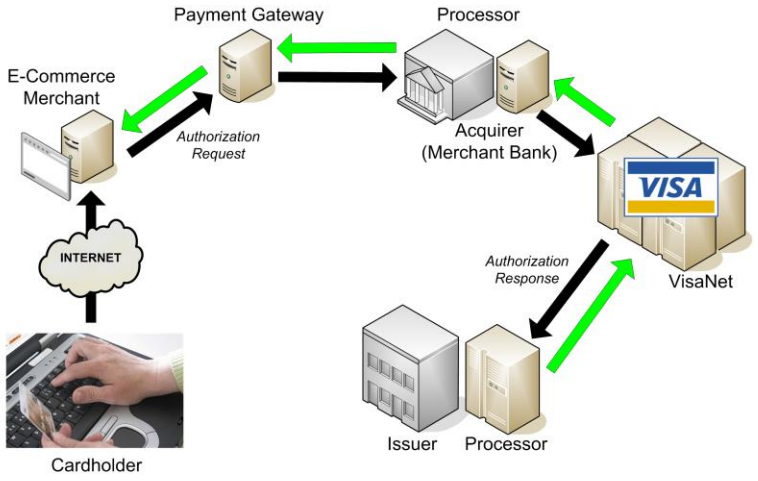
Υπονομευμένη οντότητα	Αρχικό Πρόστιμο (€)	Αποτυχία συμβατότητας			
		Μετά από 90 μέρες	Μετά από 4 μήνες	Μετά από 5 μήνες	Κάθε επακόλουθο μήνα
Έμποροι Επιπέδου 1 (>6M)	€50,000	€30,000	€50,000	€75,000	€75,000
Έμποροι Επιπέδου 2 (1 – 6M)	€25,000	€15,000	€25,000	€50,000	€50,000
Έμποροι Επιπέδου 3 (e-commerce μόνο 20,000 – 1M)	€10,000	€5,000	€10,000	€15,000	€15,000
Έμποροι Επιπέδου 4	€10,000 (€2,500)	€5,000	€10,000	€15,000	€15,000
VisaNet Processors/Μέλος Processors	€50,000	€30,000	€50,000	€75,000	€75,000
Έμποροι Processor	€25,000	€15,000	€25,000	€30,000	€30,000
Άλλοι	€10,000	€5,000	€10,000	€25,000	€25,000

Take a quite modest compromise of 10,000 cards at a merchant, you could expect to have compromise fees of 5 euros per card; investigation costs of about 30,000 euros; an average fraud of 1,000 euros per card, card replacement costs of 20 euros per card; and 30 euros per card in chargeback fees. That comes to around 11 million euros – and 10,000 is a small example.

Ποιους αφορά το PCI DSS;



Ποιους αφορά το PCI DSS;



Διαδικασίες πιστοποίησης PCI DSS

- **Ευθύνη των Acquirers**
- Οι Acquirers πρέπει να ελέγξουν τους εμπόρους, ανάλογα με το επίπεδο που έχουν καταταχθεί, για το αν έχουν όλα τα έγγραφα για την πιστοποίηση συμβατότητας με το PCI DSS.

- Οι Acquirers πρέπει να καταθέτουν μηνιαία αναφορά στην Visa και όλα τα έγγραφα για την πιστοποίηση συμβατότητας με το PCI DSS πρέπει να είναι άμεσα διαθέσιμα στη Visa, εάν αυτά ζητηθούν βεβαίως.

Διαδικασίες πιστοποίησης PCI DSS

- **Οι διαδικασίες πιο αναλυτικά:**

- Τρίμηνη δικτυακή ανάλυση επικινδυνότητας από πιστοποιημένο ASV (Approved Scanning Vendor).

- Ετήσιο επιτόπιο έλεγχο ασφαλείας πληροφορικής (On-Site PCI Data Security Assessment) από πιστοποιημένο QSA (Qualified Security Assessor).

- Ετήσιο PCI ερωτηματολόγιο συμβατότητας (PCI Self-Assessment Questionnaire), που αποδεικνύει πως υπάρχει εσωτερική μέριμνα για την ασφάλεια των πληροφοριακών υποδομών της εταιρείας.