# Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων

Μαρία Καρύδα
Τμήμα Μηχανικών
Πληροφοριακών και Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Πανεπιστήμιο Αιγαίου

## Στόχοι του Κεφαλαίου

- Το Κεφάλαιο αυτό στοχεύει στην απάντηση των εξής ερωτημάτων:
  - Τι είναι οι Πολιτικές Ασφάλειας ΠΣ και για ποιους λόγους τις χρειαζόμαστε;
  - Πώς μπορούμε να αναπτύξουμε μια Πολιτική Ασφάλειας ΠΣ και τι θα πρέπει να περιλαμβάνει;
  - Ποιοι παράγοντες συμβάλλουν στην αποτελεσματική εφαρμογή μιας Πολιτικής Ασφάλειας ΠΣ;

Πανεπιστήμιο Αιγαίου

## Διαχείριση Ασφάλειας ΠΣ: **Διαδικασίες και Πρακτικές**

- Η Διαχείριση της Ασφάλειας ΠΣ στοχεύει στην προστασία των ΠΣ, περιορίζοντας την επικινδυνότητα σε αποδεκτό επίπεδο. Περιλαμβάνει συνοπτικά τις ακόλουθες διαδικασίες:
  - 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

3

Πανεπιστήμιο Αιγαίου

## Η έννοια της Πολιτικής Ασφάλειας ΠΣ

- Η Πολιτική Ασφάλειας των Πληροφοριακών Συστημάτων περιλαμβάνει το σκοπό και τους στόχους της ασφάλειας, οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν την προστασία των ΠΣ του οργανισμού
- Η Πολιτική Ασφάλειας διατυπώνεται σε ένα έγγραφο, το οποίο θα πρέπει να γνωρίζουν και να εφαρμόζουν όλοι οι χρήστες των ΠΣ

4

## Μέτρα Ασφάλειας και Σχέδιο Ασφάλειας

Πανεπιστήμιο Αιγαίου

- Οι οδηγίες και οι διαδικασίες που περιλαμβάνονται στην Πολιτική Ασφάλειας υλοποιούνται με την εφαρμογή των μέτρων προστασίας ή ασφάλειας (security measures, security controls)
- Η Πολιτική Ασφάλειας, μαζί με το σύνολο των μέτρων προστασίας, αποτελούν το Σχέδιο Ασφάλειας (Security Plan) για τα πληροφοριακά συστήματα ενός οργανισμού.

5

## Γιατί εφαρμόζουμε μια Πολιτική Ασφάλειας; 1(2)

Πανεπιστήμιο Αιγαίου

- …γιατί χρειαζόμαστε ένα συστηματικό και ολοκληρωμένο πλαίσιο που θα καθοδηγήσει την υλοποίηση των μέτρων ασφάλειας
- …γιατί λειτουργεί ως το μέσο για την επικοινωνία των εμπλεκομένων στα ζητήματα ασφάλειας (χρήστες, διοίκηση, διαχειριστές συστημάτων κλπ.)
- …γιατί δε διαθέτουμε απεριόριστους πόρους (σε χρήματα, χρόνο, ανθρώπινο δυναμικό)

6

## Γιατί εφαρμόζουμε μια Πολιτική Ασφάλειας; 2(2)

Πανεπιστήμιο Αιγαίου

και

- …γιατί έτσι θεμελιώνεται η σημασία της ασφάλειας του ΠΣ για όλα τα μέλη του οργανισμού
- …γιατί συμβάλλει στη δημιουργία κουλτούρας ασφάλειας
- …γιατί σε ορισμένες περιπτώσεις αποτελεί νομική υποχρέωση
- …γιατί αποτελεί παράγοντα εμπιστοσύνης στις σχέσεις του οργανισμού με συνεργαζόμενους φορείς και πελάτες

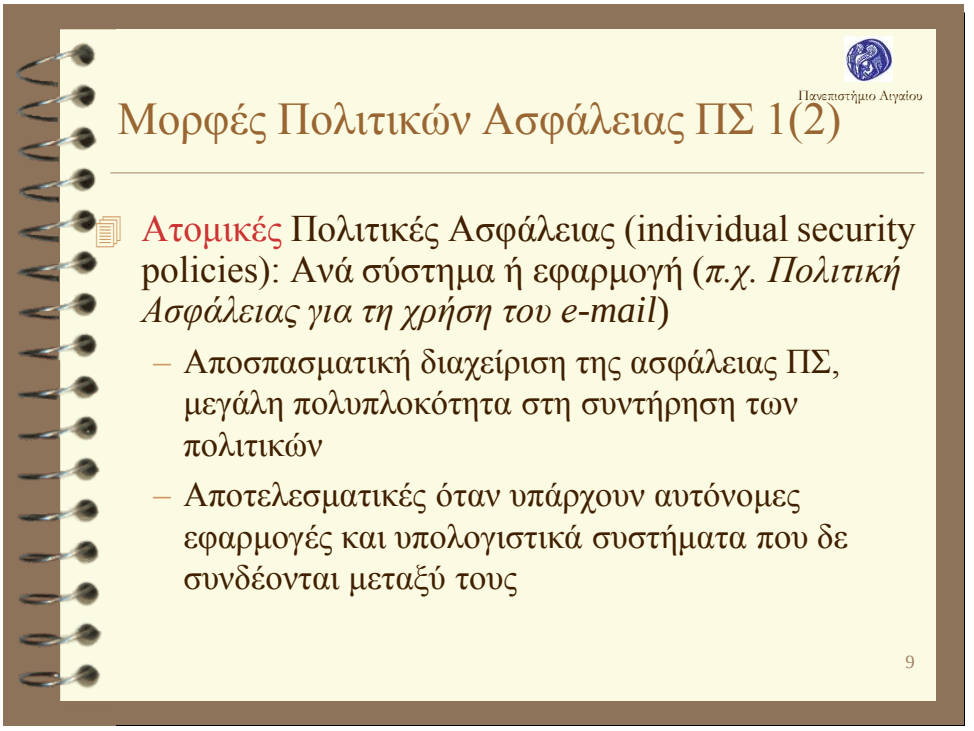
7

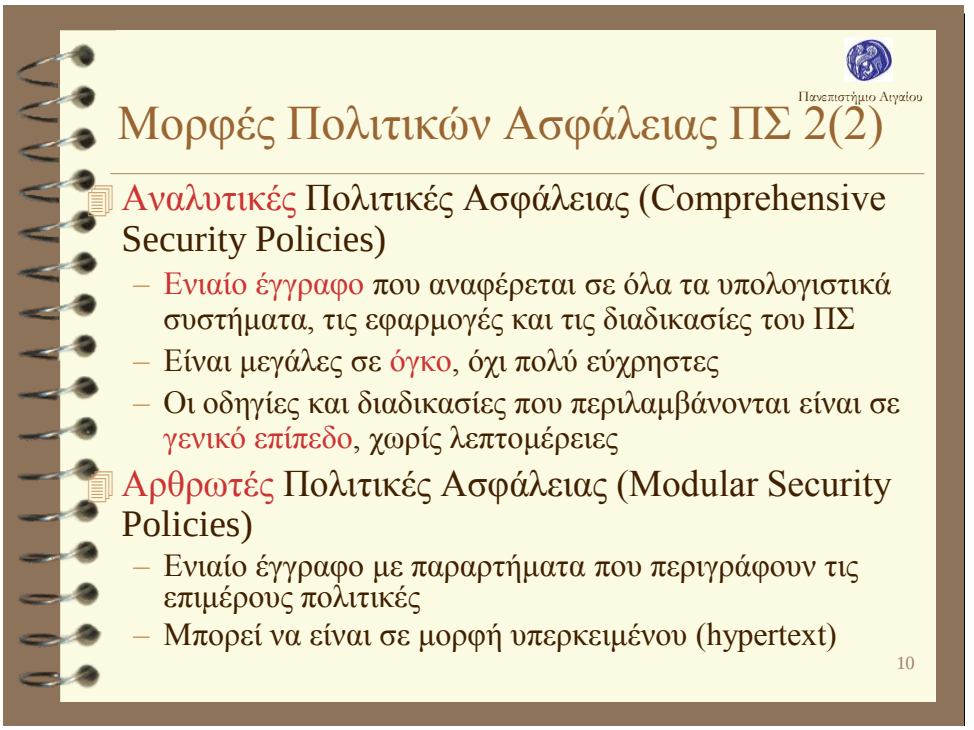
## Είδη Πολιτικών Ασφάλειας

Πανεπιστήμιο Αιγαίου

- Τεχνικές Πολιτικές Ασφάλειας (computer-oriented)
  - Πολιτικές Ασφάλειας Πληροφοριών
    - Υλοποιούν συγκεκριμένους κανόνες πρόσβασης στα δεδομένα, όπως διακριτικό έλεγχο προσπέλασης (Discretionary Access Control) ή υποχρεωτικό έλεγχο προσπέλασης (Mandatory Access Control).
  - Πολιτικές Ασφάλειας Λειτουργικών Συστημάτων
  - Πολιτικές Ασφάλειας Δικτύων Υπολογιστών
- Οργανωσιακές Πολιτικές Ασφάλειας (human-oriented)
  - Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων

8


Πανεπιστήμιο Αιγαίου
Μορφές Πολιτικών Ασφάλειας ΠΣ 1(2)
Ατομικές Πολιτικές Ασφάλειας (individual security policies): Ανά σύστημα ή εφαρμογή (π.χ. Πολιτική Ασφάλειας για τη χρήση του e-mail)
– Αποσπασματική διαχείριση της ασφάλειας ΠΣ, μεγάλη πολυπλοκότητα στη συντήρηση των πολιτικών
– Αποτελεσματικές όταν υπάρχουν αυτόνομες εφαρμογές και υπολογιστικά συστήματα που δε συνδέονται μεταξύ τους
9


Πανεπιστήμιο Αιγαίου
Μορφές Πολιτικών Ασφάλειας ΠΣ 2(2)
Αναλυτικές Πολιτικές Ασφάλειας (Comprehensive Security Policies)
– Ενιαίο έγγραφο που αναφέρεται σε όλα τα υπολογιστικά συστήματα, τις εφαρμογές και τις διαδικασίες του ΠΣ
– Είναι μεγάλες σε όγκο, όχι πολύ εύχρηστες
– Οι οδηγίες και διαδικασίες που περιλαμβάνονται είναι σε γενικό επίπεδο, χωρίς λεπτομέρειες
Αρθρωτές Πολιτικές Ασφάλειας (Modular Security Policies)
– Ενιαίο έγγραφο με παραρτήματα που περιγράφουν τις επιμέρους πολιτικές
– Μπορεί να είναι σε μορφή υπερκειμένου (hypertext)
10

Πανεπιστήμιο Αιγαίου

## Πηγές Απαιτήσεων Ασφάλειας

- Οι απαιτήσεις για την ασφάλεια του ΠΣ που πρέπει να ικανοποιεί η Πολιτική Ασφάλειας προέρχονται από όλους τους εμπλεκόμενους στη χρήση και λειτουργία του ΠΣ ενός οργανισμού, όπως είναι:
  - Οι χρήστες και διαχειριστές των ΠΣ
  - Η διοίκηση του οργανισμού
  - Οι πελάτες του οργανισμού
  - Οι νομικές και κανονιστικές διατάξεις που διέπουν τη λειτουργία του

11

Πανεπιστήμιο Αιγαίου

## Ανάπτυξη Πολιτικών Ασφάλειας 1(2)

- Για να διαμορφώσουμε μια Πολιτική Ασφάλειας ΠΣ πρέπει να αξιολογήσουμε, κατ'αρχήν, το επίπεδο της ασφάλειάς του. Για το σκοπό αυτό, μπορούμε να χρησιμοποιήσουμε:
  - Μεθόδους Ανάλυσης Επικινδυνότητας (π.χ. SBA, MARION, CRAMM)
  - Πρότυπα διαχείρισης της ασφάλειας των ΠΣ (π.χ. ISO 17799, GMITS)

12

Πανεπιστήμιο Αιγαίου

## Ανάπτυξη Πολιτικών Ασφάλειας 2(2)

- Η Πολιτική Ασφάλειας ΠΣ που αναπτύσσουμε θα πρέπει να περιλαμβάνει απαντήσεις στα ακόλουθα ερωτήματα:
  - Ποιος είναι ο σκοπός και ποιοι οι στόχοι της Πολιτικής;
  - Ποια είναι τα αγαθά του ΠΣ που χρειάζονται προστασία;
  - Ποιοι είναι οι υπεύθυνοι για την προστασία των αγαθών αυτών και ποιες είναι οι αρμοδιότητές τους;
  - Ποιο είναι το εύρος και ποια τα όρια εφαρμογής της;
  - Πώς θα γίνεται ο έλεγχος της εφαρμογής της;
  - Ποια είναι τα χρονικά πλαίσια που ισχύει η Πολιτική;

13

Πανεπιστήμιο Αιγαίου

## Περιεχόμενο Πολιτικών Ασφάλειας ΠΣ

- Οι οδηγίες και τα μέτρα προστασίας που καθορίζει η πολιτική ασφάλειας ΠΣ θα πρέπει να καλύπτουν τις ακόλουθες κατηγορίες απαιτήσεων ασφάλειας:
  - Ζητήματα Προσωπικού
  - Φυσική Ασφάλεια
  - Έλεγχος Πρόσβασης στο ΠΣ
  - Διαχείριση Υλικού και Λογισμικού
  - Νομικές υποχρεώσεις
  - Διαχείριση της Πολιτικής Ασφάλειας
  - Οργανωτική Δομή
  - Σχέδιο Συνέχισης Λειτουργίας

14

## Περιεχόμενο Πολιτικής Ασφάλειας ΠΣ 1(8): **Ζητήματα Προσωπικού**

- Στόχος των οδηγιών και των μέτρων ασφάλειας που ανήκουν σε αυτή την κατηγορία είναι η μείωση της επικινδυνότητας που οφείλεται σε ανθρώπινα λάθη, απάτη, κλοπή ή κατάχρηση των πόρων του ΠΣ. Αναφέρονται κυρίως σε:
  - Ρόλους και υπευθυνότητες για την προστασία των αγαθών του ΠΣ
  - Διαδικασίες επιλογής νέου προσωπικού
  - Εκπαίδευση και ενημέρωση των χρηστών
  - Αντιμετώπιση και αναφορά περιστατικών παραβίασης της ασφάλειας

15

## Περιεχόμενο Πολιτικής Ασφάλειας ΠΣ 2(8): **Φυσική Ασφάλεια**

- Τα μέτρα που υποστηρίζουν τη φυσική ασφάλεια έχουν ως κύριο στόχο την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στους χώρους του ΠΣ και της καταστροφής των αγαθών του. Αναφέρονται κυρίως σε:
  - Έλεγχο φυσικής πρόσβασης σε κρίσιμους χώρους (π.χ. Server room)
  - Προστασία της υγείας των χρηστών (safety)

16

## Περιεχόμενο Πολιτικής Ασφάλειας ΠΣ 3(8): **Έλεγχος Πρόσβασης**

- Η πρόσβαση των χρηστών του ΠΣ στις πληροφορίες, τα υπολογιστικά συστήματα και τις εφαρμογές θα πρέπει να καθορίζεται με βάση τις επιχειρηματικές ανάγκες και τις απαιτήσεις ασφάλειας.
- Συχνά εφαρμόζεται η αρχή "*need to know*" για την απονομή δικαιώματος πρόσβασης στους χρήστες.

17

## Περιεχόμενο Πολιτικής Ασφάλειας ΠΣ 4(8): **Διαχείριση Υλικού και Λογισμικού**

- Προμήθεια και Συντήρηση Υλικού
  - Οι οδηγίες αυτές στοχεύουν στη διατήρηση του επιθυμητού επιπέδου ασφάλειας, προσδιορίζοντας τις διαδικασίες για την αγορά και τη συντήρηση του υλικού (π.χ. απαίτηση προμήθειας πιστοποιημένων προϊόντων)
- Ανάπτυξη και Συντήρηση Λογισμικού
  - Οι οδηγίες που περιλαμβάνονται πρέπει να καλύπτουν τις ακόλουθες περιπτώσεις:
    - Αγορά έτοιμων προϊόντων (πακέτων λογισμικού) από εξωτερικούς προμηθευτές
    - Ανάπτυξη και συντήρηση λογισμικού από αναδόχους
    - Εσωτερική ανάπτυξη και συντήρηση των εφαρμογών

18

## Περιεχόμενο Πολιτικής Ασφάλειας ΠΣ 5(8): **Νομικές Απαιτήσεις**



- Συμμόρφωση με το νομικό και κανονιστικό πλαίσιο, όπως:
  - Ο Νόμος 2472/1997 για την *Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα*.
  - Οι νόμοι για την προστασία των πνευματικών δικαιωμάτων
  - Οι αποφάσεις των Ανεξάρτητων Διοικητικών Αρχών, όπως η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

19

## Περιεχόμενο Πολιτικής Ασφάλειας ΠΣ 6(8): **Διαδικασίες Διαχείρισης της Πολιτικής Ασφάλειας**



- Η Πολιτική Ασφάλειας θα πρέπει να προσδιορίζει και τις απαιτούμενες δραστηριότητες για την εφαρμογή της, που αφορούν:
  - Την αξιολόγηση και αναθεώρηση της Πολιτικής
  - Τον έλεγχο εφαρμογής της (audit) και τον καθορισμό των ενεργειών που προβλέπονται στις περιπτώσεις μη τήρησής της από τους χρήστες

20

## Περιεχόμενο Πολιτικής Ασφάλειας ΠΣ 7(8): **Οργανωτική Δομή**

- Για να εφαρμοστεί η Πολιτική Ασφάλειας θα πρέπει να υπάρχει η αντίστοιχη οργανωτική και διοικητική δομή
  - Δημιουργία των κατάλληλων ρόλων και κατανομή υπευθυνοτήτων (π.χ. Υπεύθυνος Ασφάλειας)
  - Δημιουργία διαδικασιών για τον εντοπισμό και την αναφορά περιστατικών παραβίασης της ασφάλειας



## Περιεχόμενο Πολιτικής Ασφάλειας ΠΣ 8(8): **Σχέδιο Συνέχισης Λειτουργίας**

- Ειδικά στις περιπτώσεις κρίσιμων ΠΣ, η Πολιτική Ασφάλειας πρέπει να περιλαμβάνει οδηγίες που αφορούν στις απαιτούμενες ενέργειες μετά την πραγματοποίηση ενός σημαντικού περιστατικού παραβίασης της ασφάλειας, ώστε οι λειτουργίες του οργανισμού να εξακολουθήσουν να πραγματοποιούνται με κάποιους εναλλακτικούς τρόπους, έως ότου αντιμετωπιστεί το πρόβλημα ασφάλειας του ΠΣ (π.χ. να υπάρχει εφεδρικό web site).

Πανεπιστήμιο Αιγαίου

## Χαρακτηριστικά Πολιτικών Ασφάλειας ΠΣ 1(2)

- Όταν αναπτύσσουμε μια Πολιτική Ασφάλειας, επιδιώκουμε τα ακόλουθα:
  - Οι οδηγίες και τα μέτρα προστασίας να καλύπτουν το σύνολο των αγαθών του ΠΣ και όλες τις λειτουργίες του (πληρότητα)
  - Να λάβουμε υπόψη τις τρέχουσες τεχνολογικές εξελίξεις (επικαιρότητα)
  - Με κάποιες τροποποιήσεις ή προσθήκες να μπορεί η Πολιτική να καλύπτει μικρές αλλαγές ή επεκτάσεις στο ΠΣ (γενικευσιμότητα)

23

Πανεπιστήμιο Αιγαίου

## Χαρακτηριστικά Πολιτικών Ασφάλειας ΠΣ 2(2)

…και πρέπει να λαμβάνουμε υπόψη ότι

- η 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)

24

## Διαμόρφωση Πολιτικών Ασφάλειας ΠΣ: **Προσεγγίσεις**

Πανεπιστήμιο Αιγαίου

- Ανάλογα με τον οργανισμό και το ΠΣ για το οποίο αναπτύσσουμε μια Πολιτική Ασφάλειας, μπορούμε να ακολουθήσουμε:
  - Την προσέγγιση της υποχρεωτικής εφαρμογής:
    - επιτρεπτές ενέργειες θεωρούνται μόνον εκείνες που προβλέπονται και προδιαγράφονται στην Πολιτική Ασφάλειας
  - Την προσέγγιση του διακριτικού ελέγχου:
    - όλες οι ενέργειες που δεν περιλαμβάνονται στις απαγορευμένες θεωρούνται επιτρεπτές και σύμφωνες με την πολιτική
  - Την προσέγγιση της κατά περίπτωση εφαρμογής:
    - οι οδηγίες ασφάλειας της Πολιτικής θεωρούνται υποχρεωτικές, υπάρχει όμως η δυνατότητα να παρακαμφθούν κατά περίπτωση

25

## Εφαρμογή Πολιτικών Ασφάλειας ΠΣ: **Παράγοντες Επιτυχίας** 1(2)

Πανεπιστήμιο Αιγαίου

- 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

26

Πανεπιστήμιο Αιγαίου

## Εφαρμογή Πολιτικών Ασφάλειας ΠΣ: **Παράγοντες Επιτυχίας** 2(2)

…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

27

Πανεπιστήμιο Αιγαίου

## Αναθεώρηση των Πολιτικών Ασφάλειας ΠΣ

- Το περιεχόμενο και οι διαδικασίες εφαρμογής της Πολιτικής Ασφάλειας θα πρέπει να αναθεωρούνται:
  - Σε τακτικά χρονικά διαστήματα (Τακτικές αναθεωρήσεις)
  - Έπειτα από σημαντικά περιστατικά παραβίασης της ασφάλειας, ουσιώδεις αλλαγές στο υλικό ή το λογισμικό, επέκταση ή διασύνδεση του ΠΣ με άλλα συστήματα (Έκτακτες αναθεωρήσεις)

28

# Σύνοψη

- Η Πολιτική Ασφάλειας ΠΣ αποτελεί το βασικό εργαλείο για τη διαχείριση της ασφάλειας των ΠΣ
- Η ανάπτυξη μιας Πολιτικής απαιτεί την καταγραφή, σε ένα έγγραφο, των βασικών στόχων της ασφάλειας, μαζί με τους τρόπους και τα μέσα επίτευξης των στόχων αυτών
- Το περιεχόμενο, η μορφή και ο τρόπος εφαρμογής μιας Πολιτικής μπορεί να διαφοροποιηθούν ανάλογα με τον οργανισμό και το ΠΣ
- Η αποτελεσματική εφαρμογή της εξαρτάται, μεταξύ άλλων, από την υποστήριξη και συμμετοχή της διοίκησης, τη σταδιακή εφαρμογή και τη συμβολή της Πολιτικής στην επίτευξη των στόχων του οργανισμού

29