

# Πρόγραμμα Πιστοποίησης Γνώσεων & Δεξιοτήτων ECDL Core+ IT Security

Εξεταστέα Ύλη (Syllabus)



---

Έκδοση 1.0  
[www.ecdl.gr](http://www.ecdl.gr)

**PEOPLECERT Hellas A.E - Φορέας Πιστοποίησης Ανθρώπινου Δυναμικού**  
Κοραή 3, 105 64 Αθήνα, Τηλ.: 210 372 9100, Fax: 210 372 9101, e-mail: [info@peoplecert.org](mailto:info@peoplecert.org), [www.peoplecert.org](http://www.peoplecert.org)

**Πνευματικά Δικαιώματα © 2010 Ίδρυμα ECDL (ECDL Foundation - [www.ecdl.org](http://www.ecdl.org))**

Όλα τα δικαιώματα είναι κατοχυρωμένα. Κανένα μέρος αυτού του εγγράφου δεν μπορεί να αναπαραχθεί κατά οποιονδήποτε τρόπο, εκτός αν υπάρχει σχετική άδεια από το Ίδρυμα ECDL. Για άδεια αναπαραγωγής του υλικού θα πρέπει να απευθυνθείτε στον εκδότη. Η επίσημη Εξεταστέα ύλη του ECDL Web Editing έκδοση 2.0, είναι αυτή που δημοσιεύει το Ίδρυμα ECDL και μπορεί να βρεθεί στη διεύθυνση δικτυακού τόπου: <http://www.ecdl.org>.

**ΑΠΟΚΥΡΗΞΗ:** Παρ' όλα τα μέτρα που έχουν ληφθεί από το Ίδρυμα ECDL για την προετοιμασία αυτής της έκδοσης, καμία εγγύηση δεν παρέχεται από το Ίδρυμα ECDL, ως εκδότη, για την πληρότητα των πληροφοριών που περιέχονται εντός αυτής. Επίσης, το Ίδρυμα ECDL δεν είναι υπεύθυνο ή υπόχρεο για οποιαδήποτε απώλεια, βλάβη, φθορά, οποιουδήποτε μεγέθους προκύψει λόγω πληροφοριών, οδηγιών ή συμβουλών που περιέχονται σε αυτό το έγγραφο.

Το Ίδρυμα ECDL διατηρεί το δικαίωμά του να πραγματοποιεί αλλαγές μονομερώς και κατά τη διακριτική του ευχέρεια οποτεδήποτε χωρίς προηγούμενη γνωστοποίηση.

ECDL Foundation is a registered business name of The European Computer Driving License Foundation Limited and ECDL Foundation (International) Limited. European Computer Driving License, ECDL, International Computer Driving License, IC DL, and related logos are all registered Trade Marks of ECDL Foundation. All rights reserved.

## ΕΞΕΤΑΣΤΕΑ ΥΛΗ (SYLLABUS)

### Ασφάλεια Πληροφοριακών Συστημάτων

The official version of IT Security Syllabus Version 1.0 is the version published on the ECDL Foundation website: [www.ecdl.org](http://www.ecdl.org)

### **Disclaimer**

Although every care has been taken by The European Computer Driving Licence Foundation Ltd. (hereinafter referred to as ECDL Foundation) in the preparation of this publication, no warranty is given by ECDL Foundation as publisher as to the completeness of the information contained within it and neither shall ECDL Foundation be responsible or liable for any errors, omissions, inaccuracies, loss or damage whatsoever arising by virtue of such information or any instructions or advice contained within this publication. Changes may be made by ECDL Foundation at its own discretion and at any time without notice.

### **Copyright © 2010 ECDL Foundation**

All rights reserved. No part of this publication may be reproduced in any form except as permitted by ECDL Foundation. Enquiries for permission to reproduce material should be directed to ECDL Foundation.

## ECDL / ICDL Ενότητα 12 – Ασφάλεια Πληροφοριακών Συστημάτων (IT Security)

Τα ακόλουθα αποτελούν την Εξεταστέα Ύλη για την *ECDL / ICDL Ενότητα 12, Ασφάλεια Πληροφοριακών Συστημάτων (Module 12, IT Security)*. Η Εξεταστέα Ύλη περιγράφει, μέσω μαθησιακών στόχων, τις γνώσεις και τις δεξιότητες που θα πρέπει να κατέχει ένας υποψήφιος της ενότητας *ECDL/ICDL Ενότητα 12, Ασφάλεια Πληροφοριακών Συστημάτων (IT Security)*. Επίσης, η Εξεταστέα Ύλη παρέχει/συνιστά το υπόβαθρο για τη θεωρητική και την πρακτική εξέταση σε αυτήν την ενότητα.

### Στόχοι της Ενότητας

Η ενότητα *ECDL/ICDL Ενότητα 12, Ασφάλεια Πληροφοριακών Συστημάτων (IT Security)* απαιτεί από τον υποψήφιο να κατανοεί τις κύριες έννοιες που διέπουν την ασφαλή χρήση των Τεχνολογιών Πληροφορίας και Επικοινωνιών (Πληροφορικής και Επικοινωνιών - ΤΠΕ) στην καθημερινή ζωή καθώς και να χρησιμοποιεί τις σχετικές τεχνικές και εφαρμογές που απαιτούνται για την υλοποίηση και συντήρηση ασφαλών συνδέσεων δικτύου, την ασφαλή σύνδεση στο Διαδίκτυο, καθώς και τη σωστή διαχείριση δεδομένων και πληροφοριών. Οι υποψήφιοι της ενότητας θα εφοδιαστούν με τις κατάλληλες γνώσεις και δεξιότητες για ασφαλή εργασία με τις ΤΠΕ και θα μπορούν να ανταποκρίνονται επάξια στις κοινές προκλήσεις ασφαλείας κατά την χρήση των ΤΠΕ.

Ο υποψήφιος θα πρέπει να είναι σε θέση να:

- Κατανοεί τις βασικές έννοιες που αφορούν τη σημασία της ασφαλούς διατήρησης πληροφοριών και δεδομένων, της φυσικής ασφάλειας των δεδομένων, της προστασίας των προσωπικών δεδομένων και της κλοπής ταυτότητας (identity theft).
- Προστατεύει έναν υπολογιστή, μια συσκευή ή ένα δίκτυο από λογισμικό κακόβουλης χρήσης (malware) και από μη εξουσιοδοτημένη πρόσβαση σε αυτά (unauthorised access).
- Κατανοεί τους τύπους δικτύων, τους τύπους σύνδεσης καθώς και ειδικά θέματα δικτύων, συμπεριλαμβανομένων και αυτών που σχετίζονται με τα τείχη προστασίας (firewalls).
- Περιηγείται στον Παγκόσμιο Ιστό (World Wide Web) και να επικοινωνεί μέσω Διαδικτύου (Internet) με ασφάλεια.
- Κατανοεί τα θέματα ασφαλείας που σχετίζονται με την επικοινωνία, συμπεριλαμβανομένων και των θεμάτων που αφορούν το ηλεκτρονικό ταχυδρομείο (e-mail) και την ανταλλαγή άμεσων μηνυμάτων (instant messaging).
- Δημιουργεί αντίγραφα ασφαλείας (backup) και να επαναφέρει (restore) δεδομένα σωστά και με ασφάλεια καθώς και να διαθέτει/κατανέμει δεδομένα και συσκευές με ασφάλεια.

ΚΑΤΗΓΟΡΙΑ	ΓΝΩΣΤΙΚΗ ΠΕΡΙΟΧΗ	ΑΝΑΦ.	ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
12.1 Έννοιες Ασφαλείας	12.1.1 Απειλές κατά των Δεδομένων (Data Threats)	12.1.1.1	Κατανόηση της διαφοράς μεταξύ δεδομένων και πληροφοριών.
		12.1.1.2	Κατανόηση του όρου ηλεκτρονικό έγκλημα/έγκλημα στον κυβερνοχώρο (cybercrime).
		12.1.1.3	Κατανόηση της διαφοράς μεταξύ hacking (πληροφορική πειρατεία - εισβολών σε μη εξουσιοδοτημένα δίκτυα για αναγνώριση – αναφορά αδυναμιών ασφαλείας), cracking (εισβολών σε δίκτυα για κακόβουλη χρήση, όπως υποκλοπή κωδικών, σπάσιμο προγραμμάτων) και ethical hacking (εξουσιοδοτημένη εισβολή σε δίκτυα για αναγνώριση και αναφορά αδυναμιών ασφαλείας).
		12.1.1.4	Αναγνώριση απειλών κατά των δεδομένων από ανωτέρα βία, όπως: φωτιά, πλημμύρες, πόλεμος, σεισμός.
		12.1.1.5	Αναγνώριση απειλών κατά των δεδομένων από: τους εργαζόμενους, τους παρόχους υπηρεσιών και άτομα εκτός εταιρείας.
	12.1.2 Αξία της Πληροφορίας	12.1.2.1	Κατανόηση των λόγων προστασίας προσωπικών στοιχείων/πληροφοριών, όπως: αποφυγή κλοπής ταυτότητας (identity theft), ηλεκτρονική απάτη.
		12.1.2.2	Κατανόηση των λόγων προστασίας εμπορικώς ευαίσθητων στοιχείων/πληροφοριών, όπως: πρόληψη κλοπής ή κακής χρήσης των στοιχείων ενός πελάτη, οικονομικών στοιχείων.
		12.1.2.3	Προσδιορισμός μέτρων πρόληψης μη-εξουσιοδοτημένης πρόσβασης σε δεδομένα, όπως: κρυπτογράφηση (encryption), χρήση κωδικών πρόσβασης (passwords).
		12.1.2.4	Κατανόηση βασικών χαρακτηριστικών ασφάλειας πληροφοριών, όπως: εμπιστευτικότητα (confidentiality), ακεραιότητα (integrity), διαθεσιμότητα (availability).
		12.1.2.5	Προσδιορισμός των κύριων απαιτήσεων προστασίας, διατήρησης και ελέγχου δεδομένων/ιδιωτικότητας στη χώρα σας.
12.1.2.6		Κατανόηση της σημασίας δημιουργίας και τήρησης οδηγιών και πολιτικών για τη χρήση των ΤΠΕ.	

ΚΑΤΗΓΟΡΙΑ	ΓΝΩΣΤΙΚΗ ΠΕΡΙΟΧΗ	ΑΝΑΦ.	ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
	12.1.3 Προσωπική Ασφάλεια	12.1.3.1	Κατανόηση του όρου κοινωνική μηχανική (social engineering) καθώς και των συνεπειών της, όπως: συλλογή πληροφοριών, ηλεκτρονική απάτη, πρόσβαση σε υπολογιστικό σύστημα.
		12.1.3.2	Προσδιορισμός μεθόδων κοινωνικής μηχανικής, όπως: τηλεφωνικές κλήσεις, ηλεκτρονική υφαρπαγή προσωπικών δεδομένων (phishing), κρυφοκοίταγμα (shoulder surfing).
		12.1.3.3	Κατανόηση του όρου κλοπή στοιχείων ταυτότητας (identity theft) και των επιπτώσεών της: προσωπικές, οικονομικές, επιχειρηματικές, νομικές.
		12.1.3.4	Προσδιορισμός μεθόδων κλοπής στοιχείων ταυτότητας, όπως: ανάκτηση δεδομένων από διάφορα έγγραφα – πχ πεταμένους λογαριασμούς (information diving), ηλεκτρονική υφαρπαγή δεδομένων, αποθηκευμένων σε μαγνητικά μέσα, όπως τραπεζικές κάρτες, και δημιουργία κλωνοποιημένων καρτών ή «ξάφρισμα» (skimming), δημιουργία ψευδών συνθηκών για απόσπαση δεδομένων/πληροφοριών (pretexting).
	12.1.4 Ασφάλεια Αρχείων	12.1.4.1	Κατανόηση της επίδρασης της ενεργοποίησης/απενεργοποίησης των ρυθμίσεων ασφαλείας μακροεντολών.
		12.1.4.2	Ορισμός κωδικού πρόσβασης (password) σε αρχεία, όπως: έγγραφα, συμπιεσμένα αρχεία, υπολογιστικά φύλλα.
		12.1.4.3	Κατανόηση των πλεονεκτημάτων και των περιορισμών της κρυπτογράφησης (encryption).
	12.2 Λογισμικό Κακόβουλης Χρήσης (Malware)	12.2.1 Ορισμός και Λειτουργία	12.2.1.1
12.2.1.2			Αναγνώριση διάφορων μεθόδων απόκρυψης του κακόβουλου λογισμικού, όπως: Δούρειοι ίπποι (Trojans), ιών σε επίπεδο λειτουργικού συστήματος (rootkits) και κερκόπορτες/πίσω πόρτες” (back doors).
12.2.2 Τύποι / Είδη		12.2.2.1	Αναγνώριση διάφορων τύπων μολυσματικών κακόβουλων λογισμικών και κατανόηση της λειτουργίας τους, όπως: ιοί (viruses), σκουλήκια (worms).

ΚΑΤΗΓΟΡΙΑ	ΓΝΩΣΤΙΚΗ ΠΕΡΙΟΧΗ	ΑΝΑΦ.	ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
		12.2.2.2	Αναγνώριση τύπων κλοπής δεδομένων, κερδοσκοπικού/εκβιαστικού κακόβουλου λογισμικού και κατανόηση της λειτουργίας τους, όπως: λογισμικό ανεπιθύμητης διαφήμισης (adware), λογισμικό παρακολούθησης (spyware), δίκτυα μολυσμένων υπολογιστών (botnets), καταγραφείας πληκτρολογίου (keystroke logging) και λογισμικό ανεπιθύμητων κλήσεων (diallers).
	12.2.3 Προστασία	12.2.3.1	Κατανόηση του πώς λειτουργεί το λογισμικό προστασίας από ιούς (anti-virus) και των περιορισμών του.
		12.2.3.2	Σάρωση συγκεκριμένης μονάδας δίσκου, συγκεκριμένων φακέλων ή αρχείων χρησιμοποιώντας λογισμικό προστασίας από ιούς. Προγραμματισμός σάρωσης χρησιμοποιώντας ένα λογισμικό προστασίας από ιούς.
		12.2.3.3	Κατανόηση του όρου καραντίνα (quarantine) και της επίπτωσης της απομόνωσης μολυσμένων/ύποπτων αρχείων.
		12.2.3.4	Κατανόηση της σημασίας λήψης και εγκατάστασης ενημερώσεων, αρχείων ορισμών ιών του λογισμικού προστασίας από ιούς.
12.3 Ασφάλεια Δικτύου	12.3.1 Δίκτυα	12.3.1.1	Κατανόηση του όρου δίκτυο και αναγνώριση των συνήθων τύπων δικτύου, όπως: Τοπικό Δίκτυο (Local Area Network - LAN), Δίκτυο Ευρείας Περιοχής (Wide Area Network - WAN), Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network - VPN).
		12.3.1.2	Κατανόηση του ρόλου του διαχειριστή δικτύου (network administrator) στη διαχείριση της ταυτοποίησης (authentication), της εξουσιοδότησης (authorisation) και των λογαριασμών (accounting) των χρηστών σ' ένα δίκτυο.
		12.3.1.3	Κατανόηση της λειτουργίας και των περιορισμών ενός τείχους προστασίας (firewall).
	12.3.2 Συνδέσεις Δικτύου	12.3.2.1	Αναγνώριση των επιλογών σύνδεσης σε δίκτυο, όπως: μέσω καλωδίου / ενσύρματα (cable), ασύρματα (wireless).

ΚΑΤΗΓΟΡΙΑ	ΓΝΩΣΤΙΚΗ ΠΕΡΙΟΧΗ	ΑΝΑΦ.	ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
		12.3.2.2	Κατανόηση ότι ο τρόπος σύνδεσης σ' ένα δίκτυο έχει επιπτώσεις για την ασφάλεια, όπως: κακόβουλο λογισμικό, πρόσβαση σε δεδομένα χωρίς άδεια, διατήρηση ιδιωτικότητας.
	12.3.3 <i>Ασύρματη Ασφάλεια</i>	12.3.3.1	Αναγνώριση της σημασίας ύπαρξης κωδικού ασφαλείας για την προστασία της ασύρματης πρόσβασης στο δίκτυο.
		12.3.3.2	Αναγνώριση των διαφορετικών τύπων ασύρματης προστασίας / κρυπτογράφησης, όπως: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Media Access Control (MAC).
		12.3.3.3	Επίγνωση ότι η μη-προστατευμένη χρήση ενός ασύρματου δικτύου μπορεί να επιτρέψει σε υποκλοπείς (wireless eavesdroppers) να έχουν πρόσβαση στα δεδομένα σας.
		12.3.3.4	Σύνδεση σ' ένα προστατευμένο/μη-προστατευμένο ασύρματο δίκτυο.
	12.3.4 <i>Έλεγχος Πρόσβασης</i>	12.3.4.1	Κατανόηση του σκοπού ύπαρξης λογαριασμού δικτύου και πώς η πρόσβαση μέσω αυτού πρέπει να πραγματοποιείται με χρήση ονόματος χρήστη (user name) και κωδικού πρόσβασης (password).
		12.3.4.2	Αναγνώριση ορθών πολιτικών κωδικών πρόσβασης, όπως: μη-αποκάλυψη κωδικών, τακτική αλλαγή κωδικών, επαρκές πλήθος χαρακτήρων κωδικού, κατάλληλη μίξη χαρακτήρων (γράμματα, αριθμοί και ειδικοί χαρακτήρες).
		12.3.4.3	Αναγνώριση συνήθων βιομετρικών τεχνικών ασφαλείας που χρησιμοποιούνται για τον έλεγχο πρόσβασης, όπως: δακτυλικό αποτύπωμα, σάρωση οφθαλμών.
12.4 <b>Ασφαλής Χρήση του Ιστού</b>	12.4.1 <i>Πλοήγηση στον Ιστό (Web Browsing)</i>	12.4.1.1	Επίγνωση ότι συγκεκριμένες ηλεκτρονικές δραστηριότητες (αγορές, χρηματοοικονομικές συναλλαγές) θα πρέπει να πραγματοποιούνται μόνο σε ασφαλείς ιστοσελίδες.
		12.4.1.2	Αναγνώριση μιας ασφαλούς ιστοσελίδας, όπως: https, σύμβολο κλειδαριάς (lock symbol).

ΚΑΤΗΓΟΡΙΑ	ΓΝΩΣΤΙΚΗ ΠΕΡΙΟΧΗ	ΑΝΑΦ.	ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
		12.4.1.3	Επίγνωση της διαδικασίας παραπλάνησης (pharming) δηλαδή της ανακατεύθυνσης ενός προγράμματος περιήγησης σε ψεύτικες τοποθεσίες Web χρησιμοποιώντας το Σύστημα Διαχείρισης Ονοματοδοσίας (DNS - Domain Name System).
		12.4.1.4	Κατανόηση του όρου ψηφιακό πιστοποιητικό (digital certificate). Επικύρωση ενός ψηφιακού πιστοποιητικού.
		12.4.1.5	Κατανόηση του όρου κωδικός πρόσβασης μίας χρήσης (one-time password).
		12.4.1.6	Επιλογή κατάλληλων ρυθμίσεων για την ενεργοποίηση, απενεργοποίηση της αυτόματης συμπλήρωσης, αυτόματης αποθήκευσης κατά τη συμπλήρωση μίας φόρμας.
		12.4.1.7	Κατανόηση του όρου λανθάνον αρχείο καταγραφής δεδομένων (cookie).
		12.4.1.8	Επιλογή κατάλληλων ρυθμίσεων για την αποδοχή, φραγή λανθανόντων αρχείων καταγραφής δεδομένων (cookies).
		12.4.1.9	Διαγραφή προσωπικών δεδομένων από έναν φυλλομετρητή ιστού, όπως: ιστορικό περιήγησης (browsing history), προσωρινά αποθηκευμένα αρχεία διαδικτύου (cached internet files), κωδικών ασφαλείας (passwords), λανθανόντων αρχείων καταγραφής δεδομένων (cookies), δεδομένων αυτόματης συμπλήρωσης (autocomplete data).
		12.4.1.10	Κατανόηση του σκοπού, της λειτουργίας και των τύπων του λογισμικού ελέγχου-περιεχομένου, όπως: λογισμικό φιλτραρίσματος διαδικτυακού περιεχομένου, λογισμικού γονικού ελέγχου.
	12.4.2 Κοινωνική Δικτύωση (Social Networking)	12.4.2.1	Κατανόηση της σημασίας μη-αποκάλυψης εμπιστευτικών πληροφοριών σε διαδικτυακές τοποθεσίες κοινωνικής δικτύωσης.
		12.4.2.2	Επίγνωση της ανάγκης εφαρμογής των κατάλληλων ρυθμίσεων απορρήτου σε λογαριασμούς κοινωνικής δικτύωσης.

ΚΑΤΗΓΟΡΙΑ	ΓΝΩΣΤΙΚΗ ΠΕΡΙΟΧΗ	ΑΝΑΦ.	ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ
		12.4.2.3	Κατανόηση πιθανών κινδύνων κατά τη χρήση διαδικτυακών τοποθεσιών κοινωνικής δικτύωσης, όπως: εκφοβισμός στον κυβερνοχώρο (cyber bullying), προσέγγιση πλασματικής φιλίας με απώτερο σκοπό την διαδικτυακή σεξουαλική παρενόχληση ή αποπλάνηση ανηλίκου (grooming), παραπλανητικές/επικίνδυνες πληροφορίες, ψευδείς ταυτότητες, σύνδεσμοι ή μηνύματα απάτης.
12.5 Επικοινωνίες	12.5.1 Ηλεκτρονικό Ταχυδρομείο (E-Mail)	12.5.1.1	Κατανόηση του σκοπού της κρυπτογράφησης, αποκρυπτογράφησης ενός μηνύματος ηλεκτρονικού ταχυδρομείου.
		12.5.1.2	Κατανόηση του όρου ψηφιακή υπογραφή (digital signature).
		12.5.1.3	Δημιουργία και προσθήκη μιας ψηφιακής υπογραφής.
		12.5.1.4	Επίγνωση της πιθανότητας λήψης δόλιων / απρόσμενων και αυτόκλητων μηνυμάτων.
		12.5.1.5	Κατανόηση του όρου ηλεκτρονική υφαρπαγή προσωπικών δεδομένων (phishing). Αναγνώριση των συνήθων χαρακτηριστικών της ηλεκτρονικής υφαρπαγής προσωπικών δεδομένων, όπως: χρήση ονομάτων υπαρχόντων εταιριών, ατόμων, ψευδής σύνδεσμοι διαδικτυακών τοποθεσιών.
		12.5.1.6	Επίγνωση του κινδύνου μόλυνσης του Η/Υ με κακόβουλο λογισμικό (malware) που προήλθε από άνοιγμα επισυναπτόμενου αρχείου που περιέχει μια μακροεντολή ή ένα εκτελέσιμο αρχείο.
	12.5.2 Ανταλλαγή Άμεσων Μηνυμάτων (Instant Messaging)	12.5.2.1	Κατανόηση του όρου ανταλλαγή άμεσων μηνυμάτων (instant messaging - IM) και των χρήσεών του.
		12.5.2.2	Κατανόηση των αδυναμιών ασφαλείας που σχετίζονται με τις εφαρμογές ανταλλαγής άμεσων μηνυμάτων (IM), όπως: λογισμικό κακόβουλης χρήσης (malware), πρόσβαση μέσω κερκόπορτας/"πίσω πόρτας" (backdoor access), πρόσβαση σε αρχεία.

ΚΑΤΗΓΟΡΙΑ	ΓΝΩΣΤΙΚΗ ΠΕΡΙΟΧΗ	ΑΝΑΦ.	ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ	
<b>12.6 Ασφαλή Διαχείριση Δεδομένων</b>	<i>12.6.1 Διασφάλιση και Δημιουργία Αντιγράφων Ασφαλείας Δεδομένων</i>	12.5.2.3	Αναγνώριση μεθόδων εξασφάλισης της εμπιστευτικότητας κατά τη χρήση εφαρμογών ανταλλαγής άμεσων μηνυμάτων (IM), όπως: κρυπτογράφηση (encryption), μη-αποκάλυψη σημαντικών πληροφοριών, περιορισμός στο διαμοιρασμό αρχείων (file sharing).	
		12.6.1.1	Αναγνώριση των τρόπων εξασφάλισης της φυσικής ασφάλειας συσκευών, όπως: καταγραφή της θέσης και των λεπτομερειών μιας συσκευής, χρήση καλωδίων κλειδώματος/κλειδαριές συρματόσχοινου, έλεγχος πρόσβασης.	
		12.6.1.2	Αναγνώριση της σημασίας ύπαρξης διαδικασίας δημιουργίας αντιγράφων ασφαλείας για τις περιπτώσεις απώλειας δεδομένων, οικονομικών εγγραφών, σελιδοδεικτών/ιστορικού περιήγησης διαδικτύου.	
		12.6.1.3	Προσδιορισμός των χαρακτηριστικών μιας διαδικασίας δημιουργίας αντιγράφων ασφαλείας, όπως: τακτικότητα/συχνότητα, προγραμματισμός/χρονοδιάγραμμα, τοποθεσία αποθήκευσης.	
		12.6.1.4	Δημιουργία αντιγράφων ασφαλείας δεδομένων.	
		12.6.1.5	Ανάκτηση (restore) και επικύρωση (validate) δεδομένων από αντίγραφα ασφαλείας.	
		<i>12.6.2 Ασφαλής Καταστροφή</i>	12.6.2.1	Κατανόηση του λόγου μόνιμης διαγραφής δεδομένων από μονάδες δίσκου ή άλλες συσκευές.
			12.6.2.2	Διάκριση μεταξύ διαγραφής και μόνιμης καταστροφής δεδομένων.
			12.6.2.3	Προσδιορισμός συνήθων μεθόδων μόνιμης καταστροφής δεδομένων, όπως: καταστροφή αρχείων (shredding), καταστροφή δίσκου/μέσου, απομαγνητισμός (degaussing), χρήση βοηθητικών προγραμμάτων καταστροφής δεδομένων.