PEOPLECERT

ΠΡΟΓΡΑΜΜΑ ΠΙΣΤΟΠΟΙΗΣΗΣ ΕΠΑΓΓΕΛΜΑΤΙΩΝ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΕΠΙΚΟΙΝΩΝΙΩΝ

Τεχνικός Ασφάλειας Συστημάτων Πληροφορικής

Syllabus

Μάρτιος 2017
Έκδοση 01.1

peoplecert.org

PEOPLECERT ΕΛΛΑΣ Α.Ε – Φορέας Πιστοποίησης Ανθρώπινου Δυναμικού
Κοραή 3, 105 64 Αθήνα, Τηλ.: 210 372 9100, Fax: 210 372 9101, e-mail: info@peoplecert.gr, **www.peoplecert.gr**

1. Εισαγωγή

Ο **Τεχνικός Ασφάλειας Συστημάτων Πληροφορικής** ασχολείται με την προστασία των Συστημάτων Πληροφορικής και ειδικότερα, εφαρμόζει τεχνικές που διασφαλίζουν την ακεραιότητα και τη ασφάλεια των αρχείων των υπολογιστών, των τρόπων επικοινωνίας μέσω του δικτύου και προτείνει τρόπους για τη χρήση των εφαρμογών των εταιρειών, ώστε να περιέχουν **δικλείδες ασφαλείας των πληροφοριακών συστημάτων** ενός οργανισμού. Συνεργάζεται άμεσα με τη διοίκηση της εταιρείας, προκειμένου να είναι πάντα ενήμερος για τις ανάγκες της εταιρείας και να είναι σε θέση να προτείνει εφαρμογές που θα επιτρέπουν την ασφαλή λειτουργία των συστημάτων. Το σχήμα πιστοποίησης της **PEOPLECERT** παρέχει αναγνώριση, σε διεθνές επίπεδο, για τους επαγγελματίες που καλύπτουν θέσεις, για τα οποίες απαιτείται γνώση, εξειδίκευση και εμπειρία για την εκτέλεση διάφορων ασφαλείας συστημάτων πληροφορικής όπως: διαχείριση κινδύνων προσωπικών Η/Υ και του δικτύου ενός οργανισμού, διαχείριση ασφάλειας πληροφοριών, κρυπτογράφηση και συμπίεση δεδομένων, πιστοποίηση και έλεγχος πρόσβασης, αντιμετώπιση κινδύνων και δημιουργία αντιγράφων ασφαλείας, ασφάλεια δικτύου, γνώση τοπικών και ευρωπαϊκών νόμων κλπ.

Η πιστοποίηση **Τεχνικός Ασφάλειας Συστημάτων Πληροφορικής** της **PEOPLECERT** καλύπτει τις απαιτούμενες **γνώσεις** που θα πρέπει να έχει ένας υποψήφιος για να αποδείξει μια σταθερή κατανόηση του περιεχομένου και τις απαιτήσεις των εθνικών και διεθνών πρακτικών εργασιών και αρμοδιοτήτων ασφαλείας πληροφοριακών συστημάτων ενός οργανισμού, καθώς και των απαραίτητων **δεξιοτήτων πρακτικής** εφαρμογής αυτών. Περιλαμβάνει τις κύριες και επιμέρους επαγγελματικές λειτουργίες και επαγγελματικές εργασίες οι οποίες αποτελούν το βασικό του πυρήνα και ασκούνται σε πάσης φύσεως επιχειρήσεις οργανισμούς ή φορείς, ενώ ταυτόχρονα αποτελούν προϋπόθεση για οποιαδήποτε εξειδικευμένη άσκησή του.

Συνιστάται οι υποψήφιοι προτού λάβουν μέρος στις εξετάσεις πιστοποίησης αυτού του επιπέδου, να κατέχουν τις βασικές και προχωρημένες γνώσεις που αναφέρονται στην αναλυτική εξεταστέα ύλη που ακολουθεί καθώς και να έχουν παρακολουθήσει σχετικά προγράμματα κατάρτισης και εκπαίδευσης που συνδέονται με το αντικείμενο της πιστοποίησης.

2. Σε ποιους απευθύνεται / Ακροατήριο

Η παρούσα πιστοποίηση απευθύνεται σε υφιστάμενους τεχνικούς ασφαλείας συστημάτων πληροφορικής καθώς και σε υποψήφιους που επιθυμούν να στελεχώσουν έναν οργανισμό σε μια τέτοια θέση. Απαιτείται **βασικό και προχωρημένο** επίπεδο γνώσεων και εφαρμογής των σχετικών με το αντικείμενο δεξιοτήτων για την επιτυχή απόκτηση αυτής της πιστοποίησης, αφού η πιστοποίηση σε επίπεδο **Τεχνικός Ασφάλειας Συστημάτων Πληροφορικής** της **PEOPLECERT** δηλώνει την ικανότητα του κατόχου της να ασκήσει/εκτελέσει εργασίες για τις ακόλουθες κατηγορίες εργασιών:

i. Γνώση των βασικών θεμάτων και εννοιών της ασφάλειας πληροφοριών ενός πληροφοριακού συστήματος: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα (availability), πιστοποίηση (authentication) και ταυτοποίηση (non-repudiation).
ii. Διαχείριση κινδύνων και ασφάλειας πληροφοριών
iii. Κρυπτογράφηση και πιστοποίηση και έλεγχος πρόσβασης
iv. Διαθεσιμότητα πληροφοριών και αντίγραφα ασφαλείας
v. Ασφάλεια δικτύων και τηλεπικοινωνιών
vi. Κοινωνικές, ηθικές και νομικές πτυχές της Ασφάλειας πληροφοριακών συστημάτων.

Η πιστοποίηση **Τεχνικός Ασφάλειας Συστημάτων Πληροφορικής** της **PEOPLECERT** αποδεικνύει με τον καλύτερο και πλέον αξιόπιστο τρόπο ότι ο κάτοχός της κατέχει τις απαραίτητες γνώσεις, ικανότητες και πρακτικές έτσι ώστε να είναι σε θέση να παρέχει υψηλού επιπέδου και αποδοτικότητας εργασίες ασφαλείας πληροφοριακών συστημάτων, σε υποστηρικτικό επίπεδο.

3. Μαθησιακοί στόχοι

Δεδομένου ότι η πιστοποίηση αυτή είναι επαγγελματικού επιπέδου, οι υποψήφιοι θα εκπαιδευτούν σε όλες τις σχετικές γνώσεις και δεξιότητες των τυπικών ομάδων εργασιών εφαρμογής και διατήρησης της ασφάλειας πληροφοριακών συστημάτων, έτσι ώστε να διεκπεραιώνει όλες τις αναγκαίες για τη λειτουργία του οργανισμού διοικητικές εργασίες.

Οι **κάτοχοι** της πιστοποίησης **Τεχνικός Ασφάλειας Συστημάτων Πληροφορικής** της **PEOPLECERT** θα είναι σε θέση να αποδείξουν τις γνώσεις τους, την ικανότητα, την κατανόηση και την αρμοδιότητα για την εφαρμογή όλων των απαραίτητων γνώσεων και δεξιοτήτων εκτέλεσης εργασιών ασφαλείας πληροφοριακών συστημάτων και θα είναι σε θέση να:

- Γνωρίζουν διάφορους τρόπους προστασίας δεδομένων σε επίπεδο προσωπικού Η/Υ και σε επίπεδο τοπικού δικτύου με σύνδεση στο Διαδίκτυο
- Τηρούν τον κώδικα δεοντολογίας
- Προστατεύουν τα δεδομένα μιας εταιρίας από τον κίνδυνο απώλειας, από επίθεση ιών και κακόβουλων χρηστών.
- Ρυθμίζουν τα θέματα προσβασιμότητας, διαθεσιμότητας και κρυπτογράφησης δεδομένων που διέπουν τα πληροφοριακά συστήματα ενός οργανισμού.
- Γνωρίζουν και χειρίζονται τα πιο γνωστά/διαδεδομένα εργαλεία και προγράμματα που έχουν σχεδιαστεί για την ασφάλεια πληροφοριακών συστημάτων.
- Κατέχουν γνώση και πρακτικές δεξιότητες στις εργασίες που αφορούν τη ασφάλεια ενός πληροφοριακού συστήματος.
- Παρέχουν εκτελεστική υποστήριξη λειτουργιών του οργανισμού όπως: ρύθμιση προσωπικών Η/Υ, ρύθμιση τείχους προστασίας, παρακολούθηση και έλεγχος σφαλμάτων, επιμέλεια αναφορών, δημιουργία αντιγράφων ασφαλείας, έλεγχος πρόσβασης Διαδικτύου και υπηρεσιών ηλεκτρονικού ταχυδρομείου κλπ.

4. Εξέταση

Η εξέταση για την πιστοποίηση **Τεχνικός Ασφάλειας Συστημάτων Πληροφορικής** έχει σχεδιαστεί έτσι ώστε να επικυρώνει τις γνώσεις των υποψηφίων σε σχέση τόσο επί των περιεχομένων των γνώσεων που απαιτούνται αλλά και στην εφαρμογή όλων όσων διέπουν τις εργασίες που σχετίζονται με την ασφάλεια πληροφοριακών συστημάτων.

Η εξέταση επικεντρώνεται στις παρακάτω τέσσερις κατηγορίες των γνωστικών κατηγοριών της **Ταξινομίας του Bloom (Bloom's taxonomy)**[1]:

- **Γνώση (Knowledge)**
- **Κατανόηση (Comprehension)**
- **Εφαρμογή (Apply)**
- **Ανάλυση (Analyze)**

4.1 Κριτήρια Ένταξης / Απαιτήσεις Εκπαίδευσης

Υπάρχουν συγκεκριμένα κριτήρια ένταξης στις εξετάσεις καθώς και ακαδημαϊκές, εκπαιδευτικές και επαγγελματικές απαιτήσεις για τι εξετάσεις πιστοποίησης **Τεχνικός Ασφάλειας Συστημάτων**

[1] *Η ταξινομία/κατάταξη του Bloom (Bloom's taxonomy) ορίζει **έξι** (6) επίπεδα μάθησης σε **γνωστικό επίπεδο** (γνώση, κατανόηση, εφαρμογή, ανάλυση, σύνθεση, αξιολόγηση - know, comprehend, apply, analyze, evaluate, create), τα οποία είναι σειριακά/διαδοχικά και συσωρευτικά αφού προχωρούν από το απλό προς το σύνθετο. Προκειμένου λοιπόν να επιτευχθεί το 6ο επίπεδο μάθησης, πρέπει να διασφαλιστεί ότι τα προηγούμενα πέντε επίπεδα έχουν επιτευχθεί.*

Πληροφορικής της **PEOPLECERT.**

Πιο συγκεκριμένα οι απαιτήσεις είναι οι εξής:

Ακαδημαϊκά κριτήρια	• -Απόφοιτοι Υποχρεωτικής Εκπαίδευσης, Απόφοιτοι Δευτεροβάθμιας Εκπαίδευσης, Απόφοιτοι Μεταδευτεροβάθμιας Εκπαίδευσης, Απόφοιτοι ΑΕΙ/ΤΕΙ • -ή/και διαδρομές κατάρτισης όπως αυτές προβλέπονται από την παρακολούθηση οποιουδήποτε εγκεκριμένου προγράμματος κατάρτισης στην αντίστοιχη ειδικότητα • -ή/ και πρόγραμμα κατάρτισης όπως αυτό προδιαγράφετε στο πλαίσιο του προγράμματος VOUCHER 29-64: Κατάρτιση και Πιστοποίηση Ανέργων 29-64 ετών σε κλάδους, ΕΠ Ανάπτυξη Ανθρωπίνου Δυναμικού, Εκπαίδευση και Δια βίου Μάθηση.
Βασικές δεξιότητες/γνώσεις	• Ελληνική Γλώσσα • Βασικές Γνώσεις Η/Υ • Γνώσεις Αγγλικής γλώσσας • Γνώσεις Μαθηματικών • Στοιχειώδεις Γνώσεις Διοίκησης Επιχειρήσεων

4.2 Μέθοδος Αξιολόγησης

Η μεθοδολογία της αξιολόγησης εστιάζει στις βασικές κατηγορίες Γνώση, Κατανόηση, Εφαρμογή και Ανάλυση. Η **Γνώση** (**Knowledge**) ορίζεται ως η ανάκληση υλικού και πληροφοριών που έχει ήδη μάθει κάποιος, από γεγονότα μέχρι θεωρίες και αντιπροσωπεύει το χαμηλότερο επίπεδο μαθησιακών αποτελεσμάτων στο γνωστικό τομέα. Αυτά τα μαθησιακά αποτελέσματα μετατρέπονται σε στόχους αξιολόγησης και περιλαμβάνουν γνώση και ανάκληση σε:

- Κοινές ή/και βασικές έννοιες, ορισμούς, ορολογία και αρχών επικοινωνίας
- Τυπικές απαιτήσεις και δεξιότητες ασφάλειας πληροφοριακών συστημάτων
- Διαδικασίες, κανόνες και διεργασίες ασφάλειας πληροφοριακών συστημάτων

Η **Κατανόηση** (**Comprehension**) είναι το χαμηλότερο επίπεδο αντίληψης και κατανόησης και συνεπάγεται την ικανότητα αντίληψης της σημασίας της ύλης που διδάσκεται, συμπεριλαμβανομένου και κάποιου είδους ερμηνείας, μετάφρασης ή εκτίμησης κατά τη διάρκεια της διαδικασίας. Αυτά τα μαθησιακά αποτελέσματα και στη συνέχεια και οι αντίστοιχοι στόχοι αξιολόγησης υπερβαίνουν την απλή ανάκληση πληροφοριών και μπορεί να περιλαμβάνουν:

- Κατανόηση γεγονότων, εννοιών και αρχών
- Ερμηνεία υλικού (π.χ. διαγράμματα, γραφήματα, κείμενο)
- Αιτιολόγηση μιας διαδικασίας, διεργασίας και μεθόδου αξιολόγησης

Η **Εφαρμογή** (**Application**) αφορά το επίπεδο όπου οι υποψήφιοι πρέπει να συνδυάζουν τη γνώση και την κατανόηση ενός αντικειμένου ή θέματος έτσι ώστε να είναι σε θέση να αντιληφθούν το αφηρημένο ή/και να δημιουργήσουν μία αφηρημένη έννοια (abstraction). Πιο συγκεκριμένα, οι υποψήφιοι αναμένεται να εφαρμόσουν τις γνώσεις και την κατανόησή τους έτσι ώστε να δημιουργούνται αφηρημένες/γενικότερες έννοιες, γενικές αρχές και γενικεύσεις και να εφαρμόζονται σε συγκεκριμένες **νέες** καταστάσεις. Δηλαδή, σε αυτό το επίπεδο, ο υποψήφιος μπορεί να χρησιμοποιήσει μια έννοιας ή γενίκευση σε νέες καταστάσεις και πλαίσια, και να εφαρμόσει τη γνώση από τη μάθηση/εκπαίδευση σε άλλους χώρους ή/και τομείς. Τέτοια μαθησιακά αποτελέσματα και κατά συνέπεια και οι αντίστοιχοι στόχοι αξιολόγησης υπερβαίνουν την απλή ανάκληση και κατανόηση πληροφοριών και μπορεί να περιλαμβάνουν:

- Χρήση ιδεών, αρχών και θεωριών σε νέες, ιδιαίτερες και συγκεκριμένες καταστάσεις
- Δυνατότητα επιλογής της κατάλληλης διαδικασίας, εφαρμογή αρχών και χρήση ειδικών προσεγγίσεων ή προσδιορισμός των διαθέσιμων επιλογών σε μια δεδομένη

κατάσταση
- Εφαρμογή του υλικού εκμάθησης και εκπαίδευσης σε μια νέα κατάσταση
- Εφαρμογή κανόνων, μεθόδων, εννοιών, αρχών, νόμων και θεωριών

Τα μαθησιακά αποτελέσματα σε αυτήν την κατηγορία απαιτούν ένα υψηλότερο επίπεδο κατανόησης και αντίληψης που είναι πέραν του προηγούμενου επιπέδου κατανόησης.

Η **Ανάλυση** (**Analysis**) είναι το επίπεδο μάθησης το οποίο υπερβαίνει την απλή εφαρμογή αφού απαιτείται από τους υποψήφιους να μπορούν να διασπούν τις πληροφορίες σε βασικότερα στοιχεία και να διακρίνουν τα συστατικά μιας πληροφορίας, έτσι ώστε να καταλαβαίνουν και να αντιλαμβάνονται την οργανωτική δομή της πληροφορίας και να μπορούν να κάνουν αντίστοιχες αναγωγές . Πιο συγκεκριμένα, οι υποψήφιοι θα πρέπει να διασπούν, διακρίνουν, ανιχνεύουν, ξεχωρίζουν και αναπαριστούν όλες τις σημαντικές εργασίες αυτού του επιπέδου μάθησης και συμπεριλαμβάνει και τα προηγούμενα επίπεδα γνώσης, κατανόηση και εφαρμογής. Τέτοια μαθησιακά αποτελέσματα και κατά συνέπεια και οι αντίστοιχοι στόχοι αξιολόγησης υπερβαίνουν τη γνώση, την κατανόηση και την εφαρμογή και μπορεί να περιλαμβάνουν:

- Αναγνώριση μοτίβων που χρησιμοποιούνται για την ανάλυση ενός προβλήματος
- Ανάπτυξη διαφορετικών συμπερασμάτων για την αναγνώριση/εντοπισμό κινήτρων ή αιτίων
- Εξαγωγή συμπερασμάτων
- Εύρεση στοιχείων για την υποστήριξη γενικεύσεων
- Αναγνώριση/Προσδιορισμός τμημάτων, ανάλυση των σχέσεων μεταξύ των τμημάτων και αναγνώριση των οργανωτικών αρχών που εμπλέκονται.

Τα μαθησιακά αποτελέσματα σε αυτό το επίπεδο αντιπροσωπεύουν ένα υψηλότερο πνευματικό επίπεδο από την απλή κατανόηση και εφαρμογή του υλικού αφού απαιτεί την κατανόηση τόσο του περιεχομένου όσο και της δομικής μορφής του υλικού.

Η αξιολόγηση ενσωματώνει τα παραπάνω μαθησιακά αποτελέσματα μάθησης καθώς χρησιμοποιεί αντίστοιχου στόχους της αξιολόγησης που ανταποκρίνονται στις παραπάνω γνωστικές κατηγορίες.

4.3 Μορφή Εξέτασης

Η μορφή της εξέτασης πιστοποίησης παρουσιάζεται στον παρακάτω πίνακα:

Μέθοδος	**Γραπτώς (paper based) ή Μέσω Η/Υ (web)**
Τύπος Τεστ	**1 ενιαίο τεστ** **40 ερωτήσεις Πολλαπλής Επιλογής (Multiple choice) με ή χωρίς σενάριο εργασίας (θεωρητικές και πρακτικές καταστάσεις)** *40 συνολικά βαθμοί.* *Μία δυνατή απάντηση από 4 πιθανές απαντήσεις.* *Κάθε ερώτηση λαμβάνει ένα (1) βαθμό.*
Διάρκεια	**1 ώρα (60 λεπτά)**
Βάση Επιτυχίας	**Τουλάχιστον 60% στο σύνολο του τεστ (24/40 βαθμοί)**
Επιτήρηση	**Ναι** *Φυσική επιτήρηση ή μέσω Online Proctoring*
Χρήση Βιβλίων ή άλλου Υλικού	**Όχι** *Δεν επιτρέπεται η χρήση βιβλίων ή άλλου υλικού κατά τη διάρκεια της εξέτασης.*

	Επιτρέπεται η χρήση Απλής Αριθμομηχανής με δυνατότητα εκθέτη (Calculator) εφόσον απαιτείται.
Προαπαιτούμενα	• **Ακαδημαϊκά κριτήρια** • **Βασικές δεξιότητες/γνώσεις** *όπως περιγράφονται στην ενότητα 4.1 του παρόντος εγγράφου*
Διάκριση	**ΔΕΝ Υφίσταται**

Οι ερωτήσεις προέρχονται από μια βάση ερωτήσεων (Question Test Base - QTB) που ενημερώνεται τακτικά βάσει των προδιαγραφών εξέτασης που περιγράφεται παρακάτω. Οι ερωτήσεις χρησιμοποιούνται εναλλακτικά μεταξύ διάφορων τεστ σετ. Όλα τα τεστ σετ που παράγονται έχουν τον ίδιο βαθμό δυσκολίας. Δεν ανατίθεται ποτέ το ίδιο τεστ σετ σ' έναν υποψήφιο στην περίπτωση πολλαπλών προσπαθειών στην ίδια ενότητα πιστοποίησης.

4.4 Η Εξεταστέα Ύλη Αναλυτικά

Η εξεταστέα ύλη περιλαμβάνει τις κυριότερες ενότητες που αφορούν σε σημαντικά θέματα, ομαδοποιημένα ανά κατηγορία, βάση των γνώσεων και πρακτικών εφαρμογών τους. Οι λεπτομέρειες επί των στόχων και των γνωστικών αντικειμένων ή δεξιοτήτων ανά θεματική κατηγορία, παρουσιάζονται στον παρακάτω συγκεντρωτικό πίνακα της εξεταστέας ύλης:

Τεχνικός Ασφαλείας Συστημάτων Πληροφορικής			
Κατηγορία	**Γνωστική Περιοχή**	**Αναφ**	**Γνωστική Αντικείμενο/Δεξιότητα**
1. Βασικές Έννοιες και Γνώσεις Ασφάλειας Λειτουργικότητα, πληροφοριών και δικτύων - Δεοντολογία	1.1 Διαχείριση κινδύνων	1.1.1	Γνώση των βασικών θεμάτων και εννοιών της ασφάλειας πληροφοριών: εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα (availability), πιστοποίηση (authentication), ταυτοποίησης (non-repudiation).
		1.1.2	Γνώση των βασικών αρχών που εμπλέκονται στην αποτίμηση κινδύνων (αξία πληροφοριών, ευπάθεια, απειλή, κίνδυνος, παραβίαση, επίδραση, επίπεδο κινδύνου).
		1.1.3	Γνώση των πιο βασικών κατηγοριοποιήσεων των τεχνικών μέσων ελέγχου του κινδύνου (αναγνώριση και πιστοποίηση, έλεγχος πρόσβασης, υπαιτιότητα, παρακολούθηση των λειτουργιών, επαναχρησιμοποίηση αντικειμένου, ακρίβεια, αξιοπιστία υπηρεσιών, ασφαλής ανταλλαγή δεδομένων).
		1.1.4	Γνώση των στοιχείων που μπορούν να αποκτήσουν τον έλεγχο ενός Η/Υ: λειτουργικό σύστημα, εφαρμογές, κέλυφος (shell), μακροεντολές.
		1.1.5	Γνώση των διαφορετικών τύπων υπερχείλισης (overflow) και του τρόπου χρήσης τους για εκτέλεση κώδικα. Ενημέρωση για την απομακρυσμένη παρεμβολή κώδικα (cross site scripting).
		1.1.6	Γνώση των διόδων από τις οποίες μπορεί να γίνει πρόσβαση σε έναν Η/Υ: δισκέτα, CD-ROM, μηνύματα ηλεκτρονικού ταχυδρομείου, φυλλομετρητής, πελάτες καναλιών συνομιλίας (chat clients).
	1.2 Διαχείριση Ασφάλειας και Διαθεσιμότητα Πληροφοριών	1.2.1	Γνώση του ρόλου μιας πολιτικής ασφάλειας στην καθοδήγηση διαχείρισης ασφάλειας πληροφορικών συστημάτων.

Τεχνικός Ασφαλείας Συστημάτων Πληροφορικής			
Κατηγορία	**Γνωστική Περιοχή**	**Αναφ**	**Γνωστική Αντικείμενο/Δεξιότητα**
		1.2.2	Γνώση του ποιες είναι οι βασικές διεργασίες που πρέπει να εφαρμοστούν σε ένα οργανισμό με σκοπό να επιτύχουν ασφάλεια πληροφοριών.
		1.2.3	Ενημέρωση για την ανάγκη ανάκτησης από καταστροφή και πλάνου επιχειρηματικής συνέχειας.
		1.2.4	Γνώση των ευθυνών όλων των ρόλων που εμπλέκονται σε ένα οργανισμό (προσωπικό ασφάλειας, διαχειριστές συστημάτων, χρήστες).
		1.2.5	Γνώση των κύριων σχετικών φορέων τυποποίησης (standardization bodies) και του ρόλου τους. Γνώση της ουσίας των δημοσιευμένων προτύπων (ISO/IEC 17799, BS 7799 part 2) με σκοπό το χτίσιμο μιας υποδομής διαχείρισης θεμάτων ασφάλειας μέσα σε ένα οργανισμό.
		1.2.6	Γνώση διάφορων τύπων απαιτήσεων διαθεσιμότητας πληροφοριών. Γνώση διαφόρων ειδών απαιτήσεων υποδομής στον τομέα των ICT (UPS, κλιματισμός, δομημένη καλωδίωση κλπ.).
		1.2.7	Ενημέρωση για τα διάφορα είδη μηχανισμών αναπαραγωγής πληροφορίας Σκληρών Δίσκων σε πραγματικό χρόνο (RAID - Redundant Array of Inexpensive Disks κλπ.).
		1.2.8	Πραγματοποίηση αποτελεσματικών διαδικασιών αντιγράφων ασφαλείας (τοπικά και δικτυακά). Έλεγχος αντιγράφου ασφάλειας και πραγματοποίηση ανάκτησης.
	1.3 Διαχείριση Ασφάλειας Δικτύων	1.3.1	Γνώση σχεδιασμού δικτύου και στοιχείων/συσκευών που απαρτίζουν ένα ενσύρματο/ασύρματο δίκτυο δεδομένων
		1.3.2	Γνώση των αρχών διαχείρισης ασφαλούς δικτύου δεδομένων
		1.3.3	Εφαρμογή/ρύθμιση παραμέτρων κοινών πρωτοκόλλων ασφάλειας δικτύου και συσκευών δικτύου δεδομένων
		1.3.4	Αντιμετώπιση και άρση των προβλημάτων ασφάλειας (ενσύρματων/ασύρματων) δικτύων δεδομένων
	1.4 Υποχρέωση Γνωστοποίησης	1.4.1	Γνωστοποίηση στις αρχές πιθανών ή πραγματικών κινδύνων που προέρχονται από τα αναπτυσσόμενα, σχεδιαζόμενα ή υποστηριζόμενα συστήματα
		1.4.2	Αποχή από χρήση τεχνολογιών και προϊόντων που δεν έχουν αποκτηθεί νόμιμα
		1.4.3	Εφαρμογή υφιστάμενης νομοθεσίας
		1.4.4	Τήρηση κώδικα δεοντολογίας και γνωστοποίηση στις αρχές σε περιπτώσεις μη τήρησης του
	1.5 Ποιότητα Έργου	1.5.1	Διασφάλιση λογικών και εφικτών στόχων υλοποίησης έργων
		1.5.2	Μέριμνα για την κατάλληλη γνωστική, επιστημονική και τεχνική κατάρτιση
		1.5.3	Τήρηση Επαγγελματικών Προτύπων, όταν υπάρχουν
		1.5.4	Εφαρμογή μεθόδων και προτύπων για δοκιμή, εκσφαλμάτωση και επικύρωση των αναπτυσσόμενων, σχεδιαζόμενων ή

Τεχνικός Ασφαλείας Συστημάτων Πληροφορικής			
Κατηγορία	**Γνωστική Περιοχή**	**Αναφ**	**Γνωστική Αντικείμενο/Δεξιότητα**
			υποστηριζόμενων συστημάτων και εφαρμογών
		1.5.5	Διασφάλιση της ιδιωτικότητας και της προστασίας των προσωπικών και ευαίσθητων δεδομένων
2. Πιστοποίηση και Έλεγχος Πρόσβασης	2.1 Γενικές αρχές πιστοποίησης	2.1.1	Γνώση διαφόρων σχημάτων πιστοποίησης.
		2.1.2	Γνώση των αρχών διαχείρισης συνθηματικών (password).
		2.1.3	Γνώση των αρχών πιστοποίησης Τεκμηρίου (token).
		2.1.4	Γνώση των διαφόρων σχημάτων βιομετρικής πιστοποίησης και της αποτελεσματικότητάς τους.
	2.2 Πιστοποίηση Δικτύου	2.2.1	Γνώση των διαφορετικών απαιτήσεων της πιστοποίησης δικτύου σε σχέση με την πιστοποίηση μηχανήματος (host).
		2.2.2	Γνώση των διάφορων πρωτοκόλλων για την πιστοποίηση χρηστών (PAP – Password Authentication Protocol/Πρωτόκολλο πιστοποίησης με συνθηματικά,CHAP - Challenge Handshake Authentication Protocol /Πρωτόκολλο Πιστοποίησης με πρόκληση χειραψίας).
		2.2.3	Γνώση των διάφορων πρωτοκόλλων δικτύου για πιστοποίηση δικτυακών διεργασιών.
		2.2.4	Ενημέρωση για την πολυπλοκότητα των αρχιτεκτονικών της μονής διαδικασίας πιστοποίησης (single sign-on) .
		2.2.5	Γνώση των βασικών αρχών λειτουργίας του πρωτοκόλλου Kerberos.
	2.3 Έλεγχος πρόσβασης	2.3.1	Γνώση των αρχών ελέγχου πρόσβασης.
		2.3.2	Γνώση του τι είναι μια Λίστα Ελέγχου Πρόσβασης (Access Control List – ACL)και τι μια Λίστα Δυνατοτήτων.
		2.3.3	Εξουσιοδότηση και έλεγχος λογαριασμών χρήστη
		2.3.4	Διαχείριση ελέγχου πρόσβασης σε τυπικά συστήματα αρχείων (file systems).
		2.3.5	Διαχείριση ελέγχου πρόσβασης σε ένα Σύστημα Σχεσιακής Βάσης Δεδομένων (RDBMS - Relational Data Base Management System).
		2.3.6	Εγκατάσταση, ρύθμιση και λειτουργία υπηρεσιών επικύρωσης ταυτότητας χρήστη
3. Ιοί & Κακόβουλο λογισμικό	3.1 Λογισμικό Ιών (Viral Software)	3.1.1	Γνώση των βασικών κατηγοριών λογισμικού ιών (Trojan horses -Δούρειοι Ίπποι, virus – ιοί, worms - σκουλήκια κλπ.).
		3.1.2	Γνώση των βασικών αρχών λειτουργίας προγραμμάτων προστασίας από ιούς.
		3.1.3	Γνώση των ορίων και της επικινδυνότητας των προγραμμάτων προστασίας από ιούς.
		3.1.4	Εγκατάσταση, ρύθμιση και ενημέρωση ενός προγράμματος προστασίας από ιούς.
	3.2 Κώδικας προς λήψη	3.2.1	Γνώση του τρόπου που οι εφαρμογές μπορούν να διαχειριστούν όχι μόνο κείμενο για την εκτέλεση διάφορων εντολών

Τεχνικός Ασφαλείας Συστημάτων Πληροφορικής			
Κατηγορία	**Γνωστική Περιοχή**	**Αναφ**	**Γνωστική Αντικείμενο/Δεξιότητα**
			Λειτουργικού Συστήματος αλλά να κάνουν και χρήση μακροεντολών.
		3.2.2	Γνώση του τρόπου που οι άνθρωποι μπορούν να χρησιμοποιήσουν κακόβουλα τους τύπους MIME και του πώς μπορεί να προστατευθεί ένας Η/Υ από αυτό.
		3.2.3	Γνώση του τρόπου που οι άνθρωποι μπορούν να χρησιμοποιήσουν κακόβουλα μακροεντολές και του πώς μπορεί να προστατευθεί ένας Η/Υ από αυτό.
		3.2.4	Γνώση του τρόπου που οι άνθρωποι μπορούν να χρησιμοποιήσουν κακόβουλα μικρό-εφαρμογές (applets) και του πώς μπορεί να προστατευθεί ένας Η/Υ από αυτό.
		3.2.5	Γνώση του τρόπου που το γραφικό περιβάλλον διασύνδεσης χρήστη (GUI - Graphical User Interface) μπορεί να αναγνωρίσει την ενέργεια που πρέπει να εκτελεστεί σε ένα επισυναπτόμενο αρχείο χρησιμοποιώντας τον τύπο MIME (Multi Purpose Internet Mail Extensions) και την επέκταση αρχείου.
		3.2.6	Γνώση του τρόπου που τα προγράμματα πελάτη ηλεκτρονικού ταχυδρομείου μπορούν να αναγνωρίσουν την ενέργεια που θα πρέπει να γίνει σε ένα επισυναπτόμενο αρχείο χρησιμοποιώντας τον τύπο MIME και την επέκταση αρχείου.
4. Κρυπτογράφηση	4.1 Βασικά στοιχεία κρυπτογράφησης	4.1.1	Γνώση των βασικών στοιχείων κρυπτογράφησης: συμμετρική και ασύμμετρη κρυπτογράφηση, αλγόριθμοι συμπίεσης (hashing).
		4.1.2	Συμμετρική και Ασύμμετρη κρυπτογράφηση
		4.1.3	Εξασφάλιση ασφάλειας δεδομένων μέσω κρυπτογράφησης
		4.1.4	Συναρτήσεις συμπίεσης (hash) και σύνοψης (digest)
		4.1.5	Σύγκριση μεταξύ των μεθόδων κρυπτογράφησης
	4.2 Εφαρμογή κρυπτογράφησης	4.2.1	Χρήση μεθόδων κρυπτογράφησης
		4.2.2	Εφαρμογές και κρυπτογράφηση δεδομένων
		4.2.3	Ψηφιακά πιστοποιητικά και αρχές έκδοσης

4.5 Προδιαγραφές Εξέτασης

Η εξέταση αποτελείται από ένα ενιαίο τεστ σετ, που αποτελείται από **τέσσερις** (**4**) ενότητες, σχετικές με την Εξεταστέα ύλη, με την παρακάτω δομή:

Τμήμα	Περιγραφή (Κατηγορία Εξ. Ύλης)	Τεστ (%)
1	**Βασικές Έννοιες και Γνώσεις Ασφάλειας Λειτουργικότητα, πληροφοριών και δικτύων – Δεοντολογία**	**20%**
2	**Πιστοποίηση και Έλεγχος Πρόσβασης**	**30%**
3	**Ιοί & Κακόβουλο λογισμικό**	**30%**
4	**Κρυπτογράφηση**	**20%**
	Σύνολο (40 ερωτήσεις - 40 βαθμοί)	**100%**

Οι ερωτήσεις ανάλογα με το βαθμό δυσκολίας τους έχουν διακριθεί σε: χαμηλής , μέτριας και υψηλής δυσκολίας. Η κατανομή των ερωτήσεων του τεστ επί του συνόλου των 40 ερωτήσεων ανά κατηγορία δυσκολίας είναι: **25% χαμηλής δυσκολίας, 50% μέτριας δυσκολίας και 25% υψηλής δυσκολίας.**

PEOPLECERT

PEOPLECERT - Φορέας Πιστοποίησης Προσώπων
Κοραή 3, 105 64 Αθήνα, τηλ.: 210 372 9100, Fax: 210 372 9101
www.peoplecert.gr