«Πιστοποιημένος Ειδικός στην Ασφάλεια Δεδομένων και Διαδικτύου»

Vellum Certificate in IT and Cyber Security

Syllabus / Εξεταστέα Ύλη

Vellum Global Educational Services

Έκδοση 2.0

Vellum Global Educational Services
Κεντρικά Γραφεία: Παύλου Μελά 12 / Αλεξάνδρεια / ΤΚ 59300 / Τηλ.: 2310 501895
Γραφείο Θεσσαλονίκης: Αγίου Μηνά 7 / Θεσσαλονίκη / ΤΚ 54625 / Τηλ.: 2310 531323
Γραφείο Αθήνας: Πολυτεχνείου 12 / Αθήνα / ΤΚ 10433 / Τηλ.: 210 3835114
e-mail: info@vellum.org.gr
url: https://www.vellum.org.gr

Πνευματικά Δικαιώματα

Αποκήρυξη Ευθυνών

Η Vellum Global Educational Services προετοιμάζοντας το παρόν σχήμα πιστοποίησης και διενεργώντας συστηματικούς ελέγχους ώστε να καλύπτει την εγκυρότητα του περιεχόμενού του, καμία ευθύνη δεν φέρει για οποιαδήποτε ζημία προκύψει από την χρήση του παρόντος είτε κατά τμήμα είτε κατά όλο.

Το περιεχόμενο του παρόντος είναι δυνατόν να τροποποιηθεί ή καταργηθεί όποτε κριθεί απαραίτητο και χωρίς προηγούμενη ενημέρωση.

Εξεταστέα Ύλη

Η εξεταστέα ύλη ανακοινώνεται στο δικτυακό τόπο της Vellum Global Educational Services, www.vellum.org.gr, ο οποίος είναι και ο μόνος που αναγνωρίζεται από την εταιρεία ως σημείο ενημέρωσης των ενδιαφερομένων.

Περιεχόμενα

1. Εισαγωγή

Η κυβερνοασφάλεια (Cyber Security) είναι η πρακτική προστασίας συστημάτων, δικτύων και προγραμμάτων από ψηφιακές επιθέσεις. Αυτές οι κυβερνοεπιθέσεις συνήθως στοχεύουν στην πρόσβαση, την αλλαγή ή την καταστροφή ευαίσθητων πληροφοριών, εκβίαση χρημάτων από χρήστες μέσω κακόβουλου λογισμικού, ή στο να διακόψουν τις συνήθεις επιχειρηματικές διαδικασίες.

Η εφαρμογή αποτελεσματικών μέτρων κυβερνοασφάλειας είναι ιδιαίτερα δύσκολη σήμερα, επειδή υπάρχουν περισσότερες συσκευές παρά άνθρωποι και οι εισβολείς γίνονται πιο καινοτόμοι.

Η πιστοποίηση «Πιστοποιημένος Ειδικός στην Ασφάλεια Δεδομένων και Διαδικτύου» εμβαθύνει στις τακτικές ανίχνευσης, πρόληψης και αποτροπής κυβερνοεπιθέσεων.

Η εξεταστέα ύλη και οι εξετάσεις διατίθενται στα Ελληνικά. Οι εξετάσεις είναι σχεδιασμένες ώστε να δίνουν στους υποψήφιους τη δυνατότητα να δείξουν ότι μπορούν να εφαρμόσουν τις δεξιότητες που προσδιορίζονται στην εξεταστέα ύλη.

2. Παρουσίαση του πιστοποιητικού

2.1 Σκοπός

Σκοπός του πιστοποιητικού είναι να αξιολογήσει τις γνώσεις ενός υποψηφίου σε βασικές έννοιες και λειτουργίες της κυβερνοασφάλειας.

Με την απόκτηση του «Πιστοποιημένος Ειδικός στην Ασφάλεια Δεδομένων και Διαδικτύου», ο κάτοχος αυτού θα είναι σε θέση:

- Να συντάσσει μία αξιολόγηση κινδύνου και να αναγνωρίζει τους βασικούς κινδύνους που σχετίζονται με το cloud και την εικονικοποίηση.
- Να εφαρμόζει πολιτικές ασφαλείας και τεχνικές ανάκαμψης μετά από καταστροφή.
- Να μελετά τα στατιστικά χρήσης του δικτύου με στόχο την εύρεση προβληματικών σημείων και τη βελτίωση της ασφάλειας.
- Να δημιουργεί ένα πλάνο ασφαλείας δικτύου.
- Να γνωρίζει τα βασικά στοιχεία λειτουργίας ενός δικτύου TCP/IP.
- Να σχεδιάζει ένα ασφαλές δίκτυο και να χρησιμοποιεί συστήματα ανίχνευσης και πρόληψης εισβολής.
- Να ορίζει την πρόσβαση σε ένα δίκτυο με χρήση RADIUS Server.
- Να γνωρίζει τις βασικές αρχές για την ασφάλεια ασύρματων δικτύων.
- Να αναγνωρίζει τους κινδύνους που σχετίζονται με το cloud και την εικονικοποίηση.
- Να γνωρίζει τις βέλτιστες πρακτικές για την ασφάλεια των εφαρμογών των υπολογιστών ενός δικτύου.
- Να εντοπίζει και να αφαιρεί κακόβουλο λογισμικό.

Η απόκτηση των ανωτέρω δεξιοτήτων και του πιστοποιητικού «Πιστοποιημένος Ειδικός στην Ασφάλεια Δεδομένων και Διαδικτύου», αποτελούν ανταγωνιστικό πλεονέκτημα στην αγορά εργασίας.

2.2. Στοχευόμενη ομάδα

Το «Πιστοποιημένος Ειδικός στην Ασφάλεια Δεδομένων και Διαδικτύου» απευθύνεται σε αποφοίτους λυκείου, Πανεπιστημίων ή ΤΕΙ που επιθυμούν να αποκτήσουν γνώσεις πρακτικών αποτροπής και αντιμετώπισης κυβερνοεπιθέσεων.

2.3. Δομή του πιστοποιητικού

Τα Αντικείμενα Αξιολόγησης προσδιορίζουν τις συγκεκριμένες δεξιότητες που οι υποψήφιοι πρέπει να επιδείξουν για να επιτύχουν στην εξεταστική διαδικασία. Για να προετοιμαστούν πλήρως για τις εξετάσεις, οι υποψήφιοι πρέπει να είναι σε θέση να ικανοποιήσουν όλα τα Αντικείμενα Αξιολόγησης.

Οι ενότητες που διατίθενται στο πιστοποιητικό «Πιστοποιημένος Ειδικός στην Ασφάλεια Δεδομένων και Διαδικτύου» είναι οι παρακάτω:

1: Αξιολόγηση Κινδύνου

2: Οδηγίες και Πρότυπα Δικτύωσης

3: Εποπτεία και Φροντίδα του Δικτύου

4: Εργαλεία και Υπηρεσίες για την Ασφάλεια του Δικτύου

5: Η Συλλογή Πρωτοκόλλων TCP/IP

6: Δίκτυα

7: Έλεγχος Πρόσβασης, Επαλήθευση Ταυτότητας και Εξουσιοδότηση

8: Προστασία Ασύρματων Δικτύων

9: Cloud Computing και Εικονικοποίηση

10: Ασφάλεια

11: Malware

Για να πάρει το πιστοποιητικό ο υποψήφιος θα πρέπει να επιτύχει στην εξεταστική διαδικασία πιστοποίησης, με ποσοστό επιτυχίας 70%, στο σύνολό της. Η διάρκεια της εξέτασης είναι 45΄λεπτά και το είδος ερωτήσεις πολλαπλής επιλογής.

Στις περιπτώσεις υποψηφίων με αναπηρία και ειδικές εκπαιδευτικές ανάγκες, όπως κάποιες από αυτές αναφέρονται στο Ν.3699/2008 (ΦΕΚ 199Α), η εξέταση διεξάγεται κατά περίπτωση όπως περιγράφεται πιο κάτω.

Σε κάθε περίπτωση θα πρέπει:

1. Να ενημερώσει έγκαιρα το εξεταστικό κέντρο, για να προβεί στις απαραίτητες ενέργειες ως προς τον ειδικό εξοπλισμό που ίσως χρειαστεί να προμηθευτεί, για τον δεύτερο επιτηρητή που θα πρέπει να ορισθεί, καθώς και για την εύρεση ή τον ορισμό του κατάλληλου ατόμου που θα λειτουργήσει ως βοηθός/γραφέας, ο οποίος δεν θα πρέπει να είναι ο καθηγητής του τμήματος.
2. Να προσκομίσει βεβαίωση που χορηγείται με γνωμάτευση Υγειονομικής Επιτροπής ή από Κρατικό Νοσηλευτικό Ίδρυμα ή από το αναγνωρισμένο από το Υπουργείο Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων Ιατροπαιδαγωγικό Κέντρο, στην οποία πρέπει να αναγράφεται η πάθηση.
   Συγκεκριμένα οι υποψήφιοι:

   α. που έχουν σοβαρά προβλήματα ακοής (κωφοί, βαρήκοοι) σε ποσοστό 67% και πάνω εξετάζονται κανονικά με την παρουσία ατόμου που γνωρίζει τη νοηματική μέθοδο για την παροχή οδηγιών και διευκρινήσεων προς τον εξεταζόμενο.

   β. που έχουν αδυναμία αντίληψης των χρωμάτων, όλες οι ερωτήσεις που αφορούν σε χρώματα, αναφέρονται και ονομαστικά στο ζητούμενο χρώμα. Για την ορθή απάντηση στην αντίστοιχη ερώτηση οι εξεταζόμενοι επιτρέπεται να χρησιμοποιήσουν τις ετικέτες των χρωμάτων που εμφανίζονται στα αντίστοιχα μενού.

   γ.1 που είναι τυφλοί, σύμφωνα με το ν.958/79 (ΦΕΚ 191 Α) ή έχουν ποσοστό αναπηρίας στην όρασή τους τουλάχιστον 67% ή είναι αμβλύωπες με ποσοστό αναπηρίας στην όρασή τους τουλάχιστον 67%, ή

   γ.2 έχουν κινητική αναπηρία τουλάχιστον 67% μόνιμη ή προσωρινή που συνδέεται με τα άνω άκρα, ή

   γ.3 πάσχουν από σπαστικότατα των άνω άκρων, ή

   γ.4 πάσχουν από κάταγμα ή άλλη προσωρινή βλάβη των άνω άκρων που καθιστά αδύνατη τη χρήση τους για γραφή, ή

   γ.5 παρουσιάζουν ειδικές μαθησιακές δυσκολίες όπως δυσλεξία, δυσγραφία, δυσαριθμησία, δυσαναγνωσία, δυσορθρογραφία και

   γ.6 παρουσιάζουν το φάσμα αυτισμού,

εξετάζονται σε ξεχωριστή αίθουσα με τη βοήθεια βοηθού/γραφέα. Ο βοηθός/γραφέας διαβάζει τις ερωτήσεις και πληκτρολογεί τις απαντήσεις του εξεταζόμενου.

Σημείωση: Οι υποψήφιοι της περίπτωσης γ.1 αν δεν υπάρχει εγκατεστημένο ειδικό λογισμικό (Screen Magnification Software) μπορούν να χρησιμοποιήσουν επίσης από τα Βοηθήματα των Windows τον Μεγεθυντικό Φακό. Σε όλους τους υποψηφίους παρέχεται επιπλέον χρόνος εξέτασης 30 λεπτών και αν χρειαστεί μικρό διάλειμμα.

3. Δομή και περιεχόμενο της εξεταστέας ύλης

3.1 Αντικείμενα αξιολόγησης

Τα Αντικείμενα Αξιολόγησης προσδιορίζονται από τις ενότητες, το σύνολο των οποίων αποτελεί την εξεταστέα ύλη, και προσδιορίζουν τις συγκεκριμένες γνώσεις και δεξιότητες που οι υποψήφιοι πρέπει να επιδείξουν για να επιτύχουν στην εξεταστική διαδικασία.

Οι υποψήφιοι, για να προετοιμαστούν πλήρως για τις εξετάσεις, πρέπει να μπορούν να ικανοποιήσουν όλα τα Αντικείμενα Αξιολόγησης. Κατά την εξεταστική διαδικασία όμως, μπορεί να μην εξεταστούν απευθείας όλα τα Αντικείμενα Αξιολόγησης.

Οι υποψήφιοι πρέπει να έχουν βασικές γνώσεις χειρισμού του πληκτρολογίου και του ποντικιού του υπολογιστή, καθώς η εξεταστική διαδικασία διεξάγεται με την χρήση ηλεκτρονικού υπολογιστή.

3.2 Περιεχόμενα εξεταστέας ύλης

Ενότητα 1: Αξιολόγηση Κινδύνου

- Αξιολόγηση Κινδύνου
- Εκτίμηση Κινδύνου
- Ορολογία Αξιολόγησης Κινδύνου
- Ενεργώντας για την Αξιολόγηση Κινδύνου
- Κίνδυνοι στο Cloud
- Εικονικοποίηση

Ενότητα 2: Οδηγίες και Πρότυπα Δικτύωσης

- Πολιτικές, Πρότυπα και Οδηγίες
- Εφαρμογή Πολιτικών
- Τύποι Ελέγχου & Ψευδοθετικά-Ψευδοαρνητικά
- Ανάλυση Επιπτώσεων
- Ανάκαμψη από Καταστροφή

Ενότητα 3: Εποπτεία και Φροντίδα του Δικτύου

- Εποπτεία Δικτύου
- Πλάνο Ασφαλείας
- Εποπτεία Αρχείων Καταγραφής
- Ασφάλεια Λειτουργικού Συστήματος

Ενότητα 4: Εργαλεία και Υπηρεσίες για την Ασφάλεια του Δικτύου

- Ασφαλίζοντας το Δίκτυο
- Πλάνο Ασφαλείας
- Αναφορά Ζητημάτων Ασφάλειας
- Σύγκριση Ελέγχων Ανίχνευσης και Πρόληψης

Ενότητα 5: Η Συλλογή Πρωτοκόλλων TCP/IP

- Η συλλογή πρωτοκόλλων TCP-IP
- Πρωτόκολλα και Υπηρεσίες

Ενότητα 6: Δίκτυα

- Σχεδιασμός Ενός Ασφαλούς Δικτύου
- Συσκευές Δικτύωσης
- Σύστημα Ανίχνευσης Εισβολής
- Σύστημα Ανίχνευσης Εισβολής στο Δίκτυο
- Σύστημα Πρόληψης Εισβολής στο Δίκτυο

Ενότητα 7: Έλεγχος Πρόσβασης, Επαλήθευση Ταυτότητας και Εξουσιοδότηση

- Βασικά Στοιχεία Ελέγχου Πρόσβασης
- Πρωτόκολλο RADIUS

Ενότητα 8: Προστασία Ασύρματων Δικτύων

- Ασύρματα Δίκτυα
- Αδύναμα Σημεία Ασυρμάτων Δικτύων

Ενότητα 9: Cloud Computing και Εικονικοποίηση

- Cloud Computing
- Εικονικοποίηση

Ενότητα 10: Ασφάλεια

- Ασφάλεια Εφαρμογών
- Βέλτιστες Πρακτικές

Ενότητα 11: Malware

- Malware