ΕΙΔΙΚΟ ΠΕΡΙΓΡΑΜΜΑ ΘΕΣΗΣ ΕΡΓΑΣΙΑΣ: Υπεύθυνος ασφαλείας συστημάτων και δικτύων πληροφορικής και επικοινωνιών

ΕΚΔΟΣΗ:	3
ΗΜΕΡΟΜΗΝΙΑ ΤΡΟΠΟΠΟΙΗΣΗΣ:	03/04/2026

Τομέας Πολιτικής	**Κωδικός ΓΠ**	**Τίτλος Θέσης Εργασίας**
Ψηφιακή Πολιτική και Δίκτυα Επικοινωνιών	12.4	Υπεύθυνος ασφαλείας συστημάτων και δικτύων πληροφορικής και επικοινωνιών ΤΜΗΜΑ ΑΣΦΑΛΕΙΑΣ ΥΠΟΔΟΜΩΝ - ΔΙΚΤΥΟΥ

Οργανισμός
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Μονάδα
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ | ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΣΧΕΔΙΑΣΜΟΥ | ΔΙΕΥΘΥΝΣΗ ΠΡΟΛΗΨΗΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ | ΤΜΗΜΑ ΑΣΦΑΛΕΙΑΣ ΥΠΟΔΟΜΩΝ - ΔΙΚΤΥΟΥ

Κωδικός Θέσης	**Κατηγορία Προσωπικού**
1125333221	ΠΟΛΙΤΙΚΟ ΠΡΟΣΩΠΙΚΟ

Εργασιακή Σχέση
ΜΟΝΙΜΟΙ ΥΠΑΛΛΗΛΟΙ ΤΟΥ ΔΗΜΟΣΙΟΥ /ΔΙΚΑΣΤΙΚΟΙ ΛΕΙΤΟΥΡΓΟΙ /ΔΗΜΟΣΙΟΙ ΛΕΙΤΟΥΡΓΟΙ

Εντός Προσοντολογίου	**Κατηγορία Εκπαίδευσης**	**Κλάδος**	**Ειδικότητα**
	ΠΕ	ΜΗΧΑΝΙΚΩΝ	

Τόπος Εργασίας	**Εξυπηρέτηση Πολίτη**
ΧΑΝΔΡΗ 1 & ΘΕΣΣΑΛΟΝΙΚΗΣ, 18346, ΔΗΜΟΣ ΜΟΣΧΑΤΟΥ-ΤΑΥΡΟΥ, Ελλάδα	ΝΑΙ

Συντομη Περιγραφή της θέσης εργασίας
Μεριμνά για την εφαρμογή της εγκεκριμένης πολιτικής ασφαλείας των συστημάτων & δικτύων πληροφορικής και επικοινωνιών και για την προστασία δεδομένων από μη εξουσιοδοτημένη πρόσβαση και χρήση.

Γενικό Προφίλ	
Μισθολογικές Προβλέψεις	**Βαθμός**
☑ Υπαγωγή στο μισθολόγιο	• Α΄ • Β΄ • Γ΄ • Δ΄
☐Εξαίρεση από το μισθολόγιο	
☐Επιπλέον αμοιβές	

Σχέσεις αναφοράς και συνεργασίας	
Φορείς με τους οποίους συνεργάζεται	**Αναφέρεται σε**
	• Προϊστάμενο Τμήματος ΑΣΦΑΛΕΙΑΣ ΛΟΓΙΣΜΙΚΟΥ ΚΑΙ ΑΓΑΘΩΝ ΑΣΦΑΛΕΙΑΣ (INFORMATION ASSETS) • Προϊστάμενο Διεύθυνσης ΠΡΟΛΗΨΗΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ

Κύρια καθήκοντα

- Προσδιορίζει τους στόχους της ασφάλειας και τις αντίστοιχες διαδικασίες που πρέπει να ακολουθούνται ώστε να επιτευχθούν αυτοί οι στόχοι.
- Μεριμνά για τη διασφάλιση της δυνατότητας ενός δικτύου ή συστήματος πληροφορικής και επικοινωνιών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευθεί ή μεταδοθεί, καθώς και την καλή λειτουργία των υπηρεσιών που παρέχονται ή είναι προσβάσιμες μέσω αυτού του δικτύου ή συστήματος.
- Μεριμνά για την αναγνώριση και διαχείριση κινδύνων αναφορικά με θέματα ασφαλείας.
- Ενημερώνει, ευαισθητοποιεί και εκπαιδεύει τους τελικούς χρήστες των συστημάτων & δικτύων πληροφορικής και επικοινωνιών αναφορικά με θέματα ασφαλείας.
- Αξιολογεί και εισηγείται προτάσεις στη Διοίκηση για τη βελτίωση της ασφαλείας συστημάτων & δικτύων πληροφορικής και επικοινωνιών.
- Διενεργεί ελέγχους για την επισκόπηση της ορθής εφαρμογής της πολιτικής ασφαλείας και την αποτίμηση της αποτελεσματικότητας των μέτρων ασφαλείας.
- Παρακολουθεί και ενημερώνεται τακτικά για τις ρυθμιστικές και τις τεχνολογικές εξελίξεις στο χώρο της ασφάλειας των συστημάτων & δικτύων πληροφορικής και επικοινωνιών.
- Εισηγείται και προβαίνει σε ενέργειες που αφορούν σε θέματα αρμοδιότητας του Τμήματος, όπως: (α) την αναγνώριση, την ανάλυση και την καταγραφή σε κατάλληλο και ενημερωμένο κατάλογο (μητρώο) όλων των πόρων που απαιτούνται για την παροχή ή υποστήριξη των βασικών υπηρεσιών των ΦΕΒΥ και ΠΨΥ, (β) τη διασφάλιση της ανθεκτικότητας των συστημάτων που υποστηρίζουν βασικές υπηρεσίες έναντι απειλών, με την εφαρμογή των κατάλληλων διαδικασιών δοκιμών και τεχνικών ελέγχων των ΦΕΒΥ και ΠΨΥ, σε συνεργασία με τους κατά περίπτωση αρμόδιους φορείς, (γ) τη διενέργεια των απαραίτητων ελέγχων για την προστασία του λογισμικού και των εφαρμογών στους τομείς αρμοδιότητας της Κυβερνοασφάλειας των ΦΕΒΥ και ΠΨΥ, σύμφωνα με τις απαιτήσεις ασφαλείας (ιδίως λειτουργικά συστήματα, εφαρμογές, συστήματα διαχείρισης βάσεων δεδομένων, εφαρμογές PCI, COTS), και σε συνεργασία με τους κατά περίπτωση αρμόδιους φορείς, (δ) την υποβολή προτάσεων για τη διαμόρφωση λογισμικού και εφαρμογών σε συστήματα ΤΠΕ, εφόσον ζητηθεί από τους κατά περίπτωση αρμόδιους φορείς, (ε) τον καθορισμό και την κατηγοριοποίηση των πληροφοριακών αγαθών (information assets) και την τήρηση σχετικού μητρώου – αποθετηρίου, (στ) την έκδοση κατευθυντήριων γραμμών και οδηγιών ως προς την Κυβερνοασφάλεια για την προστασία των πληροφοριακών αγαθών, σύμφωνα με τις απαιτήσεις ασφαλείας (συμπεριλαμβανομένων των απαιτήσεων ιδιωτικότητας και προστασίας των δεδομένων προσωπικού χαρακτήρα, κρυπτογράφησης, PKI, backup, DLP, διατήρηση/ καταστροφή δεδομένων).

Θεσμική Εκπροσώπιση και Συνεργασία

Απαιτούμενα Προσόντα	
Ύπαρξη ειδικών/οργανικών διατάξεων για τα απαιτούμενα τυπικά προσόντα	ΟΧΙ

Τυπικά Προσόντα	
άρθρο 5 και 27 π.δ. 50/2001	• Προσόν διορισμού στον εισαγωγικό βαθμό ορίζεται το ομώνυμο ή • ταυτόσημο κατά περιεχόμενο ειδικότητας, πτυχίο ή δίπλωμα ΑΕΙ της • ημεδαπής ή ισότιμο αντίστοιχης ειδικότητας σχολών της αλλοδαπής.
Γνώσεις	• Γνώση μεθοδολογίας και τεχνικών ανάλυσης επικινδυνότητας. • Γνώση προτύπων, τεχνικών και διαδικασιών ασφαλείας συστημάτων & δικτύων πληροφορικής και επικοινωνιών. • Βασικές γνώσεις περί το δίκαιο της πληροφορίας (ασφάλεια πληροφοριών, πληροφοριακών συστημάτων και δικτύων, ειδικά ζητήματα προστασίας προσωπικών δεδομένων). • Άριστη γνώση της αγγλικής γλώσσας (έμφαση σε τεχνική ορολογία). Συνεκτιμούμενη και η γνώση άλλων ξένων γλωσσών • Μεταπτυχιακός τίτλος σπουδών στους τομείς της Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων ή/και Ασφάλεια Δικτύων ή/και Πληροφορικής • Πιστοποιήσεις εκπαιδεύσεων σε θέματα πληροφορικής • Γνώσεις management και διαχείρισης κινδύνων-κρίσεων • Γνώση επιχειρησιακού περιβάλλοντος του φορέα.
Ειδικές απαιτήσεις θέσης Εργασίας	• Υπηρεσιακές μετακινήσεις στο εσωτερικό ή/και στο εξωτερικό • Υποχρεωτική διαβάθμιση για τη διαχείριση εμπιστευτικών / απόρρητων εγγράφων.
Εμπειρία	

Δεξιότητες	
Δεξιότητα	**Επιθυμητό επίπεδο**
ΔΙΑΧΕΙΡΙΣΗ ΓΝΩΣΗΣ	Υψηλό
ΕΠΑΓΓΕΛΜΑΤΙΣΜΟΣ & ΑΚΕΡΑΙΟΤΗΤΑ	Μέτριο
ΕΠΙΛΥΣΗ ΠΡΟΒΛΗΜΑΤΩΝ & ΔΗΜΙΟΥΡΓΙΚΟΤΗΤΑ	Υψηλό
ΗΓΕΤΙΚΟΤΗΤΑ	Μέτριο
ΟΜΑΔΙΚΟΤΗΤΑ	Μέτριο
ΟΡΓΑΝΩΣΗ & ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ	Μέτριο
ΠΡΟΣΑΝΑΤΟΛΙΣΜΟΣ ΣΤΟ ΑΠΟΤΕΛΕΣΜΑ	Μέτριο
ΠΡΟΣΑΝΑΤΟΛΙΣΜΟΣ ΣΤΟΝ ΠΟΛΙΤΗ	Χαμηλό
ΠΡΟΣΑΡΜΟΣΤΙΚΟΤΗΤΑ	Μέτριο
Επιθυμητά Προσόντα	

Διάρκεια θητείας	**Υποχρεωτική επιμόρφωση πριν την ανάληψη της θέσης**	**Άλλες Πληροφορίες**
	ΟΧΙ	