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

ΕΚΔΟΣΗ:	3
ΗΜΕΡΟΜΗΝΙΑ ΤΡΟΠΟΠΟΙΗΣΗΣ:	26/09/2024

Τομέας Πολιτικής	Κωδικός ΓΠ	Τίτλος Θέσης Εργασίας
Ψηφιακή Πολιτική και Δίκτυα Επικοινωνιών	12.4	Υπεύθυνος ασφαλείας συστημάτων και δικτύων πληροφορικής και επικοινωνιών ΤΜΗΜΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Οργανισμός
ΙΝΣΤΙΤΟΥΤΟ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΕΚΔΟΣΕΩΝ ΔΙΟΦΑΝΤΟΣ

Μονάδα
ΔΙΟΙΚΗΤΙΚΟ ΣΥΜΒΟΥΛΙΟ | ΠΡΟΕΔΡΟΣ | ΔΙΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ, ΕΦΑΡΜΟΓΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ | ΤΜΗΜΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Κωδικός Θέσης	Κατηγορία Προσωπικού
4959111821	ΠΟΛΙΤΙΚΟ ΠΡΟΣΩΠΙΚΟ

Εργασιακή Σχέση
ΙΔΙΩΤΙΚΟΥ ΔΙΚΑΙΟΥ ΑΟΡΙΣΤΟΥ ΧΡΟΝΟΥ

Εντός Προσοντολογίου	Κατηγορία Εκπαίδευσης	Κλάδος	Ειδικότητα
ΝΑΙ	ΠΕ	ΜΗΧΑΝΙΚΩΝ	ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Τόπος Εργασίας	Εξυπηρέτηση Πολίτη
Ν. ΚΑΖΑΝΤΖΑΚΗ & ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗ & ΙΤΥΕ «ΔΙΟΦΑΝΤΟΣ» ΠΑΤΡΩΝ, 26504, ΔΗΜΟΣ ΠΑΤΡΕΩΝ, Ελλάδα	ΌΧΙ

Συντομη Περιγραφή της θέσης εργασίας
Αναπτύσσει και εφαρμόζει τις δημόσιες πολιτικές του Τμήματος Κυβερνοασφάλειας

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**
• Φορείς του Δημοσίου που σχετίζονται με τα θέματα αρμοδιότητας της Διεύθυνσης • Λοιπές οργανικές μονάδες του φορέα	• Προϊστάμενος μονάδας: ΔΙΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ, ΕΦΑΡΜΟΓΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Κύρια καθήκοντα

- Προϊσταται του Τμήματος Κυβερνοασφάλειας της ΔιΠΕΚ, το οποίο είναι αρμόδιος ιδίως για:
- τη λειτουργία του Κέντρου Επιχειρησιακής Ασφάλειας του Οργανισμού.
- τη διαχείριση και εποπτεία των συστημάτων (πληροφοριακών και δικτυακών) που επιβάλουν τους κανόνες πρόσβασης και επηρεάζουν την κυβερνοασφάλεια (όπως firewall rules, ορισμός DMZs, κανόνες και διαδικασίες πρόσβασης στα συστήματα και τις εφαρμογές του Ι.Τ.Υ.Ε.).
- να προτείνει κάθε μέτρο που κρίνει απαραίτητο για την αποτροπή περιστατικών κυβερνοασφάλειας. Για το σκοπό αυτό συντονίζει τη διαχείριση όλων των συστημάτων εφαρμογής κανόνων πρόσβασης.
- την τελική έγκριση για την απομόνωση/αποκλεισμό από την πρόσβαση στο δίκτυο και τις υποδομές του Ι.Τ.Υ.Ε. οποιασδήποτε εφαρμογής, εξοπλισμού, συστήματος, υπηρεσίας, ή χρήστη που δεν τηρεί τις διαδικασίες και τους κανόνες κυβερνοασφάλειας για ασφαλή πρόσβαση και χρήση των πληροφοριακών συστημάτων, υπηρεσιών, υποδομών και δικτύων που λειτουργούν στον οργανισμό.
- Τον συντονισμό για την παρακολούθηση, αποτροπή, ανίχνευση, έρευνα και απόκριση σε απειλές και περιστατικά κυβερνοασφάλειας, οριζόντια για ολόκληρο τον Οργανισμό.
- τον σχεδιασμό, τις ελάχιστες προδιαγραφές, τον συντονισμό και εφαρμογή υπηρεσιών και συστημάτων ενίσχυσης της ασφάλειας.
- την επίβλεψη της κεντρικής διαχείρισης και συνολικής αντιμετώπισης περιστατικών κυβερνοασφάλειας των δικτύων επικοινωνίας και των πληροφοριακών συστημάτων, που συνδέονται στο δίκτυο του Οργανισμού.
- Τον προγραμματισμό διενέργειας ελέγχων και την ενίσχυση ασφάλειας εντός και εκτός του Οργανισμού.
- την αξιολόγηση μηχανισμών προστασίας και την παροχή συμβουλευτικών υπηρεσιών για την ενίσχυση της ασφάλειας.
- την υποβολή προτάσεων για τη δημιουργία πολιτικών ασφάλειας και την επίβλεψη της υλοποίησής τους.
- το σχεδιασμό και υλοποίηση δράσεων για την ενίσχυση και παρακολούθηση της ασφάλειας, με έμφαση στην ενίσχυση του αισθήματος ασφάλειας στους πολίτες και στην ενίσχυση της εμπιστοσύνης των εκπαιδευτικών, των μαθητών και των γονέων στα ψηφιακά μέσα και το διαδίκτυο.
- την επικοινωνία και τον συντονισμό μεταξύ Εθνικών και Διεθνών Κέντρων Επιχειρησιακής Ασφάλειας και Αντιμετώπισης Κυβερνοπεριστατικών.
- τη συμμετοχή στη δημιουργία και εφαρμογή των κοινοτικών και εθνικών μέτρων, που αφορούν στην ασφάλεια των δικτύων και των πληροφοριών και τη συμμετοχή σε Εθνικές και Ευρωπαϊκές ασκήσεις κυβερνοασφάλειας.
- τον σχεδιασμό και την ανάπτυξη καινοτόμων υπολογιστικών υποδομών, εργαλείων και μεθόδων για την έρευνα σε θέματα κυβερνοασφάλειας.
- Ελέγχει τη σωστή λειτουργία των Συστημάτων και Εφαρμογών που χρησιμοποιεί το Τμήμα και μεριμνά για την ενημέρωση/ανανέωση/αναβάθμισή τους σύμφωνα με τις εκάστοτε προσθήκες και αλλαγές που προκύπτουν.
- Παρακολουθεί να τηρούνται στα Πληροφοριακά Συστήματα οι διαδικασίες που επιβάλλει το ISO27001, IS27701 και GDPR, και οι διαδικασίες του ΙΤΥΕ.
- Μεριμνά για τη λειτουργική διασύνδεση των αρμοδιοτήτων με τους επιχειρησιακούς στόχους της ΔιΠΕΚ και του Οργανισμού.
- Συγκεντρώνει, επεξεργάζεται, συνθέτει και παρουσιάζει τα απαραίτητα δεδομένα για την υποστήριξη της διαδικασίας λήψης αποφάσεων.

- Παρέχει εμπεριστατωμένες εισηγήσεις στον Προϊστάμενο του, σε θέματα που άπτονται των αρμοδιοτήτων του Τμήματός του και τη ΔιΠΕΚ.
- Εισηγείται για τη συνεχή βελτίωση του τρόπου λειτουργίας του Τμήματος που προϊσταται με την υποβολή προτάσεων οργανωτικού και επιχειρησιακού ανασχεδιασμού.
- Διασφαλίζει συνθήκες συνεργασίας με τα άλλα Τμήματα της ΔιΠΕΚ, άλλες δομές του φορέα και λοιπών φορέων της Δημόσιας Διοίκησης.
- Αναλαμβάνει πρωτοβουλίες για τη βελτίωση της λειτουργίας του Τμήματος.
- Εφαρμόζει και παρακολουθεί τη στοχοθεσία του Τμήματος και αναλαμβάνει πρωτοβουλίες για τη βελτίωση της αποδοτικότητας των υπαλλήλων.
- Κατανέμει το αντικείμενο στους υπαλλήλους του Τμήματος και τους παροτρύνει για την υλοποίηση των δράσεων του Τμήματος.
- Καθοδηγεί όλους τους συνεργάτες του Τμήματος που προϊσταται σε θέματα λειτουργίας, με σκοπό την αποτελεσματική αξιοποίηση και εξοικονόμηση πόρων.
- Ανιχνεύει τις επιμορφωτικές ανάγκες του προσωπικού του Τμήματος και διαμορφώνει ευκαιρίες μάθησης για το σύνολο αυτού.
- Αξιολογεί το προσωπικό σύμφωνα με το ισχύον θεσμικό πλαίσιο.
- Εισηγείται στον προϊστάμενο της ΔιΠΕΚ για ζητήματα σύστασης, τροποποίησης και κατάργησης θέσεων εργασίας και των σχετικών περιγραμμάτων θέσεων εργασίας του Τμήματος.
- Αναθέτει και συντονίζει εργασίες στους συνεργάτες του τμήματός του για την επίτευξη των επιχειρησιακών τους στόχων.
- Παροτρύνει και αξιοποιεί το προσωπικό του τμήματός του για την επίτευξη των επιχειρησιακών στόχων του τμήματός του και της Διεύθυνσης και παρακολουθεί την εξέλιξή τους.
- Αναλαμβάνει πρωτοβουλίες για τη διαχείριση κρίσεων.
- Μεριμνά για τις διοικητικές διαδικασίες του Τμήματος
- Εκπροσωπεί το Τμήμα, όπου απαιτείται.
- Συμμετέχει ενεργά στην εκπλήρωση των αρμοδιοτήτων της ΔιΠΕΚ
- Εισηγείται στρατηγικές και δράσεις και αναγνωρίζει τους κρίσιμους παράγοντες επιτυχίας για την αποτελεσματική εφαρμογή τους
- Παρέχει οδηγίες και κατευθύνσεις βάσει των επιχειρησιακών στόχων.

Θεσμική Εκπροσώπιση και Συνεργασία
Εκπροσωπεί το Τμήμα και τη Διεύθυνση όπου απαιτείται

Απαιτούμενα Προσόντα	
Ύπαρξη ειδικών/οργανικών διατάξεων για τα απαιτούμενα τυπικά προσόντα	ΟΧΙ
Τυπικά Προσόντα	
Προσόντα βάση ΠΔ 85/2022	α) Πτυχίο ή δίπλωμα Ηλεκτρονικού Μηχανικού ή Ηλεκτρονικής και Μηχανικών Υπολογιστών ή Ηλεκτρονικού Μηχανικού και Μηχανικού Υπολογιστών ή Μηχανικού Ηλεκτρονικών Υπολογιστών και Πληροφορικής ή Μηχανικού Πληροφοριακών και Επικοινωνιακών Συστημάτων Α.Ε.Ι. της ημεδαπής ή ακαδημαϊκά ισοδύναμος ή ισότιμος τίτλος αντίστοιχης ειδικότητας σχολών της αλλοδαπής. β) Η απαιτούμενη άδεια άσκησης επαγγέλματος. γ) Γνώση χειρισμού Η/Υ στα αντικείμενα: (i) επεξεργασίας κειμένων, (ii) υπολογιστικών φύλλων και (iii) υπηρεσιών διαδικτύου.
Γνώσεις	• Γνώσεις management και διαχείρισης κινδύνων-κρίσεων.

	• Καλή γνώση της αγγλικής γλώσσας (έμφαση σε τεχνική ορολογία). • Γνώσεις στο σχεδιασμό, υλοποίηση και λειτουργία Κέντρου Επιχειρησιακής Ασφάλειας (Security Operation Center-SOC). • Μεταπτυχιακός τίτλος σπουδών με αναγνωρισμένη συνάφεια • Εμπειρία στο συντονισμό ομάδων αντιμετώπισης περιστατικών κυβερνοασφάλειας • Γνώσεις στις διαδικασίες, τα εργαλεία και τις μεθόδους ενίσχυσης της κυβερνοασφάλειας. • Γνώση του νομοθετικού πλαισίου που αφορά την Κυβερνοασφάλεια. • Γνώσεις των διαδικασιών ISO27001 και GDPR • Γνώση του νομοθετικού πλαισίου που αφορά τα χρηματοδοτούμενα έργα • Γνώση της ισχύουσας νομοθεσίας ως προς τα θέματα που άπτονται των αρμοδιοτήτων της ΔιΠΕΚ. • Γνώση των διαδικασιών διοικητικής πρακτικής
Ειδικές απαιτήσεις θέσης Εργασίας	• Εργασία πέραν του τυπικού ωραρίου. • Γνώσεις στο αντικείμενο της Κυβερνοασφάλειας • Εμπειρία σε ελέγχους παρείσδυσης (penetration testing) • Γνώση στην αξιοποίηση εργαλείων κυβερνοασφάλειας • Συμμετοχή σε ασκήσεις κυβερνοασφάλειας
Εμπειρία	5 έτη εμπειρία σε θέση συναφή με το αντικείμενο του Τμήματος

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	• Μεταπτυχιακός τίτλος σπουδών με αναγνωρισμένη συνάφεια • Καλή γνώση της αγγλικής γλώσσας (έμφαση σε τεχνική ορολογία) • Εμπειρία στο συντονισμό ομάδων αντιμετώπισης περιστατικών κυβερνοασφάλειας

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