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

| | |
|---|---|
| **ΕΚΔΟΣΗ:** | 1 |
| **ΗΜΕΡΟΜΗΝΙΑ ΤΡΟΠΟΠΟΙΗΣΗΣ:** | 31/10/2025 |

| Τομέας Πολιτικής | Κωδικός ΓΠ | Τίτλος Θέσης Εργασίας |
|---|---|---|
| Ψηφιακή Πολιτική και Δίκτυα Επικοινωνιών | 12.4 | Υπεύθυνος ασφαλείας συστημάτων και δικτύων πληροφορικής και επικοινωνιών<br>Κ0202 - ΤΜΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΩΝ, ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑΣ |

| Φορέας |
|---|
| ΔΗΜΟΣ ΘΕΣΣΑΛΟΝΙΚΗΣ |

| Μονάδα |
|---|
| Κ - ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΔΙΟΙΚΗΤΙΚΩΝ ΥΠΗΡΕΣΙΩΝ \| Κ02 - ΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ \| Κ0202 - ΤΜΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΩΝ, ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑΣ |

| Κωδικός Θέσης | Εξυπηρέτηση Πολίτη |
|---|---|
| 5980925026 | ΝΑΙ |

| Διεύθυνση Εργασίας |
|---|
| ΒΑΣΙΛΕΩΣ ΓΕΩΡΓΙΟΥ Α 1, 54636, ΔΗΜΟΣ ΘΕΣΣΑΛΟΝΙΚΗΣ, Ελλάδα |

| Εργασιακή Σχέση |
|---|
| ΙΔΙΩΤΙΚΟΥ ΔΙΚΑΙΟΥ ΑΟΡΙΣΤΟΥ ΧΡΟΝΟΥ |

| Κατηγορία Προσωπικού | Εντός Προσοντολογίου |
|---|---|
| ΠΟΛΙΤΙΚΟ ΠΡΟΣΩΠΙΚΟ | ΝΑΙ |

| Κατηγορία Εκπαίδευσης | Κλάδος | Ειδικότητα |
|---|---|---|
| ΠΕ | ΠΛΗΡΟΦΟΡΙΚΗΣ | ΠΛΗΡΟΦΟΡΙΚΗΣ (SOFTWARE-HARDWARE) |

| Σύντομη Περιγραφή Θέσης |
|---|
| 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** | **Βαθμοί** |

| | |
|---|---|
| ΕΝΙΑΙΟ ΜΙΣΘΟΛΟΓΙΟ - Ν. 4354/2015 (ΦΕΚ Α' 176), ΚΕΦ. Β' | • Α΄<br>• Β΄<br>• Γ΄<br>• Δ΄ |
| ☐Επιπλέον αμοιβές | |

| **Σχέσεις αναφοράς και συνεργασίας** | |
|---|---|
| **Φορείς με τους οποίους συνεργάζεται** | **Αναφέρεται σε** |
| • Οριζόντια υποστήριξη όλων των Υπαλλήλων όλων των Υπηρεσιών του Δήμου<br>• Θεσσαλονίκης<br>• Φορείς Δημόσιου και Ιδιωτικού Τομέα | • Προϊστάμενος μονάδας: Κ0202 - ΤΜΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΩΝ, ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑΣ<br>• Προϊστάμενος μονάδας: Κ02 - ΔΙΕΥΘΥΝΣΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ |

**Κύρια καθήκοντα**

- Παρακολουθεί και ενημερώνεται τακτικά για τις ρυθμιστικές και τις τεχνολογικές εξελίξεις στο χώρο της ασφάλειας των συστημάτων & δικτύων πληροφορικής και επικοινωνιών.
- Εφαρμόζει και επικαιροποιεί την Πολιτική Ασφάλειας Πληροφοριών του Δήμου, σύμφωνα με διεθνή
- πρότυπα (ISO 27001, NIS2, GDPR).
- Παρακολουθεί και συντονίζει τη λειτουργία firewalls, IDS/IPS, antivirus, DLP και SIEM συστημάτων.
- Διενεργεί εκτιμήσεις κινδύνου (risk assessments) και προτείνει μέτρα για μετριασμό απειλών.
- Συντονίζει τη διαχείριση περιστατικών ασφάλειας (incident response) και ενημερώνει τη Διοίκηση για
- κρίσιμα περιστατικά.
- Συνεργάζεται με τη Διεύθυνση Ηλεκτρονικής Διακυβέρνησης για την ασφάλεια των υπηρεσιών e-Gov
- και των δημοτικών εφαρμογών.
- Διασφαλίζει την ανθεκτικότητα (resilience) των συστημάτων και τη διαθεσιμότητα κρίσιμων υπηρεσιών
- (disaster recovery, backup).
- Οργανώνει περιοδικούς ελέγχους συμμόρφωσης, penetration tests και awareness trainings για το
- προσωπικό.
- Συντάσσει τεχνικές μελέτες και προτάσεις για αναβάθμιση υποδομών και ενίσχυση της ασφάλειας.
- Αποτυπώνει ανάγκες, χαρτογραφεί και υλοποιεί συστήματα και δίκτυα πληροφορικής και επικοινωνιών.
- Εισηγείται προτάσεις για την εξέλιξη των συστημάτων και δικτύων πληροφορικής και επικοινωνιών, με
- γνώμονα την αύξηση της αποτελεσματικότητάς και της αποδοτικότητας λειτουργίας αυτών, καθώς και
- την ενίσχυση της ασφάλειας.
- Καταρτίζει και εφαρμόζει σχέδια επιχειρησιακής συνέχειας (Business Continuity Plans)
- Παρακολουθεί την ασφάλεια υπηρεσιών cloud και συνεργάζεται με παρόχους SaaS, PaaS και IaaS για τη
- διασφάλιση συμμόρφωσης.
- 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.

**Θεσμική Εκπροσώπηση και Συνεργασία**

| **Απαιτούμενα Προσόντα** | |
|---|---|
| Ύπαρξη Ειδικών Οργανικών Διατάξεων | ΟΧΙ |
| **Τυπικά Προσόντα** | |
| Τυπικά Προσόντα βάσει ΠΔ 85/2022 | Πτυχίο ή δίπλωμα Πληροφορικής ή Εφαρμοσμένης Πληροφορικής ή Εφαρμοσμένης Πληροφορικής με κατεύθυνση: i) Εφαρμοσμένης Πληροφορικής ή ii) Διοίκησης Τεχνολογίας ή Εφαρμοσμένης Πληροφορικής - εισαγωγική κατεύθυνση Επιστήμης και Τεχνολογίας Υπολογιστών ή Εφαρμοσμένης Πληροφορικής - εισαγωγική κατεύθυνση Πληροφοριακά Συστήματα ή Πληροφορικής και Τηλεματικής ή Επιστήμης Υπολογιστών ή Πληροφορικής και Τηλεπικοινωνιών ή Επιστήμης και Τεχνολογίας Υπολογιστών ή Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών ή Πληροφορικής με εφαρμογές στην Βιοϊατρική ή Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων ή Ψηφιακών Συστημάτων ή Επιστημών και Πολιτισμού – Κατεύθυνση Η/Υ ή Μηχανικού Ηλεκτρονικών Υπολογιστών και Πληροφορικής ή Μηχανικού Πληροφορικής και Τηλεπικοινωνιών ή Ηλεκτρολόγου Μηχανικού και Μηχανικού Υπολογιστών ή Ηλεκτρολόγου Μηχανικού και Τεχνολογίας Υπολογιστών ή Ηλεκτρολόγου Μηχανικού και Μηχανικού Η/Υ ή Ηλεκτρονικής και Μηχανικών Υπολογιστών ή Ηλεκτρονικού Μηχανικού και Μηχανικού Υπολογιστών ή Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων ή Μηχανικού Η/Υ Τηλεπικοινωνιών και Δικτύων ή Μηχανικών Πληροφορικής και Υπολογιστών ή Μηχανικού Πληροφορικής, Υπολογιστών και Τηλεπικοινωνιών ή Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων ή Τεχνολογιών Ψηφιακής Βιομηχανίας Α.Ε.Ι. της ημεδαπής ή ακαδημαϊκά ισοδύναμος ή ισότιμος τίτλος αντίστοιχης ειδικότητας σχολών της αλλοδαπής. |
| **Επιθυμητά Προσόντα** | • Αποφασίζει με υπευθυνότητα και ευελιξία.<br>• Αναλαμβάνει πρωτοβουλίες στο χειρισμό υποθέσεων / κρίσεων.<br>• Επιδεικνύει υπευθυνότητα, μεθοδικότητα και ευελιξία<br>• Διαθέτει διοικητικές και οργανωτικές ικανότητες<br>• Επιδεικνύει Συνεργατικό /Ομαδικό πνεύμα<br>•<br>• Πιστοποιήσεις: Επιθυμητή κατοχή πιστοποιήσεων όπως ISO 27001 Lead<br>• Implementer, CompTIA Security+, CEH, CISSP ή Cisco CCNP Security.<br>•<br>• Συνεχής εκπαίδευση: Επιμόρφωση σε κυβερνοασφάλεια, cloud security,<br>• data protection, incident handling τουλάχιστον ανά διετία.<br>•<br>• Συνεργασία: Ικανότητα συνεργασίας με Αρχή Προστασίας Δεδομένων,<br>• Υπουργείο Ψηφιακής Διακυβέρνησης, CERT-GR, και εξωτερικούς παρόχους<br>• υποδομών (integrators). |
| **Επιθυμητές Γνώσεις** | • Γνώση μεθοδολογίας και τεχνικών ανάλυσης επικινδυνότητας.<br>• Γνώση προτύπων, τεχνικών και διαδικασιών ασφαλείας συστημάτων & δικτύων πληροφορικής και επικοινωνιών.<br>• Βασικές γνώσεις περί το δίκαιο της πληροφορίας (ασφάλεια πληροφοριών, πληροφοριακών συστημάτων και δικτύων, ειδικά ζητήματα προστασίας προσωπικών δεδομένων).<br>• Καλή γνώση της αγγλικής γλώσσας (έμφαση σε τεχνική ορολογία). |

| | |
|---|---|
| | • Γνώση επιχειρησιακού περιβάλλοντος του φορέα.<br>• Γνώση εργαλείων διοίκησης και διαχείρισης έργων. |
| **Ειδικές απαιτήσεις θέσης Εργασίας** | • Εργασιακό καθεστώς<br>• Ενδέχεται να απαιτείται διαθεσιμότητα εκτός ωραρίου (24/7 on call) για διαχείριση<br>• κρίσιμων περιστατικών.<br>•<br>• Εξωτερική δραστηριότητα<br>• Περιοδικές επιτόπιες επιθεωρήσεις σε δημοτικά κτίρια, data rooms ή<br>• απομακρυσμένους κόμβους (VPN, WiFi, τηλεπικοινωνιακές εγκαταστάσεις). |
| **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 |

| **Διάρκεια θητείας (έτη)** | **Υποχρεωτική επιμόρφωση** | **Άλλες Πληροφορίες** |
|---|---|---|
| | | |