

## **מכרז למשרת מנהל רשת ואבטחת מידע במועצה המקומית התעשייתית נאות חובב**

**תואר המשרה:** מנהל רשת ואבטחת מידע **היקף משרה:** 100%. **דירוג/שכר:** שכר בדירוג/ דרגה בהתאם להסכם הקיבוצי של המועצה **מקום העבודה:** מועצה מקומית תעשייתית נאות חובב. **כפיפות:** מנהל אגף תפעול ולוגיסטיקה.

**כללי:** ניהול רשת המשתמשים ואבטחת המידע של הרשות המקומית בכדי להבטיח זמינות ושימוש מיטבי במערכות המידע בהתאם להוראות הדין הקיים ולנהלי הרשות המקומית ומדיניותה.

### **תיאור התפקיד ותחומי אחריות:**

1. **ניהול ותפעול רשת המשתמשים של הרשות:** אחריות להתקנה, שדרוג ועדכון של חומרה ותוכנה במערכות הרשות, טיפול ואחריות להפעלה תקינה ובצוע בדיקות סדירות של מערך הגיבויים והשחזורים ברשות, טיפול בשרתים אשר בשימוש הרשות הכולל: הקמה, תחזוקה, תיקון, החלפה, שדרוג וכיו"ב, ניהול ביצועים ותכנון הקיבולת של המחשבים והתקשורת של הרשות המקומית, ניהול והקצאה של משאבי הרשות ברשת המחשבים של הרשות המקומית, התקנה של ציוד מחשבים חדש ו/או העתקת מחשבים קיימים בתוך משרדי הרשות ו/או באתרי הרשות לרבות כל המרכיבים הנדרשים להתקנת והפעלת הציוד, תחזוקה וטיפול של ציוד המחשבים והתקשורת ברשות המקומית בתדירות המומלצת על ידי היצרן, טיפול בתקלות ברשת המשתמשים, בתוכנה ובחומרה כולל איתור התקלות, אפיון הסיבה לתקלה, קביעת אופן הטיפול וטיפול עד לפתרון הבעיה, ניהול הקשר עם ספקי החומרה והתוכנה ופיקוח על קבלת שירותים מתאימים, יישום נהלי אבטחת מידע וניהול הרשת.
2. **ניהול יישומי תוכנה:** עדכון ושדרוג תוכנות תוך הקפדה על אינטגרציה בין כל תשתיות המחשוב של הרשות, התקנה תקופתית ותחזוקה של תוכנות הגנה ואבטחת מידע, ניהול הרשאות של משתמשים הכוללת הוספה, גריעה ועדכון ההרשאות במערכות המחשוב, ניהול של תיבות הדואר האלקטרוני של המשתמשים ברשות המקומית, ניהול גיבויים וכתובת תהליכי גיבוי של המידע הממוחשב של הרשות המקומית, תאום ויישום מערך DRP (התאוששות מאסון) ברשות.
3. **תכנון מדיניות אבטחת המידע ובקרה על יישומה:** שמירה ואבטחת המידע ברשות תוך דגש על אבטחת מידע רגיש ו/או מסווג והיבטים נוספים בהתאם להוראות הדין הקיים, הגדרה ואשרור מדיניות אבטחת המידע ברשות בשיתוף מנהל מערכות המידע והנהלת הרשות, סיווג נכסי המידע לפי רמת רגישותם והגדרת בקורות אבטחת המידע הנדרשות להם, הערכת סיכוני אבטחת מידע במערכות המידע והתקשורת, עדכון פרטי הערכת הסיכונים עם שינויים משמעותיים בתהליכים במערכות המידע או באיומי אבטחת מידע, רישום מאגרי מידע ועמידה בדרישות החוק בנושא אבטחת מידע והגנת הפרטיות, הגדרת דרישות אבטחת המידע ההכרחיות ליישום בתהליך העברת המידע ברשות ואל מחוץ לרשות המקומית, הגדרת אירועי אבטחת המידע וצורת התגובה לאירועים אלה, הנחיית הנהלת הרשות המקומית בהפניית משאבים נאותים להטמעת אמצעי אבטחת מידע ולמיקוד בסקרי סיכוני אבטחת המידע במערכות המידע והתקשורת, הדרכת משתמשים בנושא אבטחת מידע, בקרה על יישום נוהלי אבטחת המידע ברשות, אחריות להחתמת עובדים חדשים ברשות המקומית בהתייחסות לאחריות העובד בכל הנוגע להיבטי אבטחת מידע, וילווה בהצהרת סודיות, כתיבת נהלים לכל תהליך המטפל בניהול, הכנסה, תפעול, תחזוקה, והוצאה של מידע ברשות המקומית בהתאם למדיניות וצרכי אבטחת המידע ברשות המקומית ויאשרם עם כתיבתם ו/או שינויים ויפעל להטמעתם.
4. **תכנון וביצוע סקרי אבטחת מידע:** ייזום סקרי אבטחת מידע של מערך מערכות המידע והתקשורת ברשות המקומית, עריכת סקרי אבטחת מידע לפני הטמעת שינויים משמעותיים או כאשר חלו שינויים במערכות המידע והתקשורת ברשות המקומית, בחינת יעילות אמצעי ההגנה שיושמו ברשות המקומית ורמת הגדרות אבטחת המידע במערכות המידע והתקשורת, ייזום מבחני חדירה במערכות המידע והתקשורת להדמיית ניסיונות פריצה ע"י פורצים מתוך ומחוץ לרשות המקומית, הגדרת בקורות פיזיות, בהתאם להערכת הסיכונים, לאבטחת המידע, וידוא כי סקרי אבטחת המידע ומבחני החדירה נערכים ע"י גורם מקצועי, עצמאי, בלתי תלוי וחיצוני לרשות המקומית.
5. **ניהול ההרשאות, ודרכי הגישה למשתמשים:** חלוקת סביבת העבודה למעגלי אבטחה/אזורים מאובטחים לפי רמות רגישות, יישום מגנונים לניהול בקורות גישה במערכות מידע והתקשורת ברשות המקומית תוך מידור מתאים של הרשאות בין הרשות לגורמים חיצוניים, קביעת אמצעי זיהוי למערכות ושירותים לצורך זיהוי המשתמש תוך הקפדה על מניעת אפשרות העתקה או שחזור פריטי המידע של הרשות המקומית, הגדרת מדיניות סיסמאות ותהליכי גישה למערכות מידע והתקשורת ברשות המקומית.

6. **תכנון ויישום תכנית התאוששות – DRP**: פיתוח תוכנית התאוששות של מערכות המידע והתקשורת ממצבי חירום ומצבי משבר ברשות, סיוע בקביעת תהליכים קריטיים שיש להפעיל במצבי משבר וחירום ברשות המקומית, בהתייחס למכלול היחידות של הרשות המקומית ובהתאם לצרכי הרשות, הקמת אתר חירום לצורך הפעלת מערך מערכות המידע והתקשורת ולגיבוי מערך הנתונים, החומרה וכיו"ב ולהפעלתו מרגע התרחשות האסון, משבר או מצב חירום.
7. **ניהול ההגנה על מערכות המידע והתקשורת**: התקנת אמצעים המצמצמים את החשיפה לניסיונות פגיעה, כולל איתור, זיהוי ומניעה, הגדרת דרישות הגיבוי למערכות המידע והתקשורת ברשות המקומית בהתאם לצרכים השונים של הרשות המקומית, בקרת איכות הגיבויים ואופן אבטחתם, מתן אישור להעברת מידע בטרם העברת המידע לגוף ציבורי.

### **תנאים מקדימים למינוי:**

1. **השכלה**: בעל תעודת טכנאי או הנדסאי.
2. **שפות**: עברית ואנגלית ברמה גבוהה.
3. **ניסיון מקצועי**:
  - ניסיון מקצועי של שלוש שנים לפחות כמנהל רשת בת שלושה שרתים לפחות ובעלת 50 משתמשי קצה ומעלה.
  - ניסיון מקצועי של שנה לפחות כמנהל או כסגן מנהל מערכות מידע, או מנהל אבטחת מידע בחברה בעלת 25 עובדים ומעלה.
4. **ניסיון ניהולי**: ניסיון בניהול של 3 עובדים לפחות, כאשר על תקופת הניהול לעלות על משך זמן של שלוש שנים לפחות.
5. **רישום פלילי**: היעדר הרשעה בעבירה שבנסיבות העניין יש עמה קלון או בעברה מהעבירות המנויות בסעיפים 5 ו-37 לחוק הגנת הפרטיות.

### **מאפייני העשייה הייחודיים בתפקיד:**

1. עבודה מול גורמים רבים ברשות ומחוצה לה.
  2. שירותיות.
  3. ריבוי משימות ועבודה בשעות בלתי שגרתיות.
  4. התמודדות עם ריבוי יישומים ומערכות מידע.
  5. חשיפה למידע רגיש.
- ✓ העמידה בתנאי הסף תיבחן בהתאם לאסמכתאות בלבד.
  - ✓ המשרה מיועדת לגברים ונשים כאחד.
  - ✓ מועמד בעל מוגבלות זכאי לקבל התאמות הנדרשות לו מחמת מוגבלותו בהליכי הקבלה לעבודה.
  - ✓ תינתן עדיפות לאוכלוסייה הזכאית לייצוג הולם.

טופסי ומסמכי המועמדות לאיוש המשרה ניתן למצוא באתר האינטרנט [www.neot-hovav.org.il](http://www.neot-hovav.org.il) את מסמכי ההצעה יש לשלוח במייל לכתובת [mihrazimHR@neho.org.il](mailto:mihrazimHR@neho.org.il) ולא יאוחר מיום **16.17.2023** בשעה **12:00** טלפון: **08-6543129**.

בברכה, ארז בדש, ראש המועצה