נספח "א" לחוזה

מפרט שירותים

במסגרת השירותים, הספק יישם את מדיניות ויעדיה של המועצה האזורית שער הנגב ("המועצה") בתחום אבטחת המידע והסייבר כמפורט להלן:

1. ריכוז נושא אבטחת המידע במועצה - הספק ישמש כ"ממונה אבטחת מידע", כמשמעו בחוק הגנת הפרטיות, והתקנות שהותקנו מכוחו, לרבות תקנות אבטחת מידע; וכסמכות המקצועית המפקחת בנושאי אבטחת מידע, הגנה על פרטיות וסייבר, המידע והנהלים הקשורים בכך במועצה, והכל בהלימה לדין החל בעניין.

2. התווית מדיניות אבטחת המידע במערכות במועצה - לרבות בקרה על יישום הנחיות, נהלי אבטחת מידע, תכניות אבטחת מידע והתאמתם לדרישות הדין בכלל, והרשות להגנת הפרטיות הפרט. לצורך כך, הספק יכין נהלים להסדרת הנושאים הבאים -

2.1 מדיניות אבטחת מידע והגנת הסייבר;
2.2 נוהל אבטחת מאגרי המידע;
2.3 מסמך הגדרות המאגר;
2.4 מסמך מיפוי מערכות המאגר;
2.5 מדיניות אבטחה פיזית וסביבתית;
2.6 מדיניות אבטחת מידע בניהול כח אדם;
2.7 מדיניות בקרת גישה;
2.8 מדיניות סיסמאות;
2.9 מדיניות ניהול אירועי אבטחת מידע;
2.10 מדיניות גישה מרחוק;
2.11 מדיניות ניהול אבטחת מידע בשרשרת האספקה;
2.12 מדיניות שימוש בהתקנים ניידים, מחשבים ניידים, וטלפונים חכמים;
2.13 מדיניות ניהול טלאים;
2.14 מדיניות הקשחת מערכות מידע;
2.15 מדיניות גיבויים;
2.16 נוהלי תגובה - נוהל תגובה לאירועי פישינג; נוהל תגובה לאירועי דלף מידע; נוהל תגובה לאירוע של מתקפות סייבר; נוהל תגובה לאירוע של חדירת נוזקה (וירוס) לרשת הארגונית או למחשב; נוהל תגובה לאירוע של חדירת נוזקת כופר (Ransomware); נוהל תגובה להשבתה של מערכות קריטית (כגון פירוול);
2.17 נוהל ביצוע תחקור דיגיטלי (Forensics) ושימור ראיות (Chain of Custody).

3. קיום הפעולות הנדרשות לשם מניעה, איתור וזיהוי פערים בתחום אבטחת המידע - באחריות הספק הזוכה לוודא בדרכים שונות, כולל ביקורות, שהנהלים נאכפים ושאין פרצות סכנות את ביטחון המידע או הפרטיות. ממשק העבודה הישיר לביצוע ממשי של הנהלים יהיה איש ה IT של המועצה. בכלל כך הדרכה של העובדים, בין אם באמצעות לומדות שונות או בצורה פרונטאלית.

4. ליווי הפרויקטים בתחום הדיגיטאלי במועצה - יבוצע תוך פיקוח על הטמעה ויישום פתרונות לאבטחת מידע. ייעוץ לגבי רכש מערכות אבטחת מידע וטכנולוגיות חדשות, לרבות בניית כתבי כמויות, מפרטים וליווי מקצועי בהליכי הרכש הרלוונטיים.

5. הכנת תכנית עבודה שנתית בתחום אבטחת מידע - על הספק הזוכה להכין ולהציג תכנית סדורה לעבודה בשגרה, לצד תכנית לצמצום פערים קיימים. על התוכנית לכלול יעדים מתוארכים, שמות של אחראיים ותיאור של כל משימה. התוכנית תוצג כתרשים גאנט.

6. התעדכנות בטכנולוגיות לאבטחת מידע במחשב, בהיבטי בטחון מידע במחשב - הספק הזוכה יהיה מעודכן בכל הדרכים המקובלות בתחום השירותים.

7. ייעוץ בתהליכי בדיקות הקבלה, ובשלבי הפריסה וההטמעה של מערכות מחשב חדשות.

8. ביצוע בקרה אחר פעילויות המחשב, למניעת פריצות למערכת ומסירת מידע מסווג לגורם בלתי מורשה, ובדיקה כי הפעילות מתנהלת בהתאם למדיניות שנקבעה. הספק הזוכה ידגום את הלוגים והרשומות של המערכת בצורה שיטתית, על מנת לוודא שבפועל לא התבצעו כניסות וחדירות שמהוות פריצה או העברת חומר ללא מורשים.

9. ייעוץ בוועדות פנימיות ובדיונים בנושא מערכות המחשוב והענן במועצה, במועדים שתקבע המועצה מפעם לפעם.

10. קביעת נהלי העבודה, המלצה על רכישת מוצרים ופתרונות אבטחה, למניעת דלף מידע בממשקים עם יחידות המועצה, וספקי שירותי אירוח.

11. מעורבות בכל תהליך ההרשאות לעובדים, על מנת לוודא כי העובדים מסווגים כנדרש. לאחר קביעת נהלים לכלל העובדים, יקבעו הרשאות ספציפיות למידע, פר-תפקידי העובדים השונים, הנדרשים לקבלתו.

12. תכנון והוצאה לפועל של ביקורות ותרגילים בתחום אבטחת המידע ליחידות המועצה השונות ולמשתמשי הקצה.

13. טיפול בהיבטי ביטחון בעת העסקת קבלנים חיצוניים בנושא המחשוב, וטיפול באבטחת המידע של פרויקטים חיצוניים.

14. ביצוע מטלות נוספות בתחום אבטחת המידע והסייבר, בהתאם להנחיות הממונה על מאגרי המידע במועצה.

15. אספקת שירותי IR (צוות תגובה לאירועי סייבר). השירות יאופיין בבצוע הפעולות הבאות -

15.1 בניית תכנית מסודרת לטיפול במתקפת סייבר, המבוססת על מערכות המחשוב במועצה ומדרג חשיבותן ;

15.2 הגדרת איש קשר יחיד, שישמש כמרכז הנתונים ותמונת המצב עבור המועצה בעת אירוע סייבר ;

15.3 בניית SLA בדירוג לזמן חירום;

15.4 ביצוע תרגילי אירוע סייבר, המדמה תקיפה, טיפול והתאוששות. בתום כל תרגול יבוצע שלב של מסקנות והמלצות;

15.5 זיהוי, בידוד הזירות הדיגיטליות שנפגעו, ובלימת המתקפה;

15.6 אטימת זירת האירוע למניעת זליגה;

15.7 ביצוע בקרות אירוע סייבר ו/או אבטחת מידע; ליווי רציף וטיפול בכל שלבי החזרת מצב לקדמותו במהירות, תוך מזעור בנזק למינימום; ביצוע תחקיר אירוע מקיף, מסקנות ונקודות לביצוע, ובסופו הגשת דוח ממצאים והמלצות להימנעות מהישנות;

15.8 בדיקת תקפות של דרישות המיגון ואבטחת המידע.

16. בשים לב למהות השירותים, אופיים וחשיבותם, אין בתיאורם במפרט זה, כדי להוות רשימה סגורה ביחס לשירותים הנדרשים, והמועצה שומרת לעצמה את הזכות להזמין מספקים אחרים, שירותים נוספים הנמצאים בתחום עיסוקו ומומחיותו של הספק הזוכה.

17. ככל שהמועצה תיזקק שירותי אבטחת מידע חורגים, שלא פורטו בחוזה ובמפרט, והספק הזוכה יסכים לבקשת המועצה לספקם, תחושב תמורת השירותים על בסיס שעות עבודה שיושקעו בפועל בצירוף תשלום עבור זמן נסיעה (כל שיידרש), לפי תעריף של 250 (מאתיים וחמישים) ₪ לכל שעת עבודה מלאה ו-100 (מאה) ₪ לכל שעת נסיעה שתבוצע, וחלק יחסי מהסכומים האמורים בגין חלק של שעה. תשלומים לפי סעיף זה ישולמו בתוספת מע"מ, במועדים, ובאופן הנקובים בחוזה.

18. האמור במפרט זה, אינו בא לגרוע מהנקוב בחוזה, אלא להוסיף על הוראותיו. ככל שתתגלה הוראה מקצועית סותרת (בלבד), תגבר זו הנקובה במפרט.

* * *