

---

**מכרז למתן שירותי הנחיה  
ותמיכה בתחום אבטחת מידע  
וסייבר עבור חברת נתיבי איילון**

---

---

**מסמך ג' – מפרט השירותים**

---

## 1 כללי

- 1.1 בחלק זה יפורטו השירותים הנדרשים מהספק.
- 1.2 השירותים הנדרשים מחולקים ל 2 סוגים:
- 1.2.1 **שירותים תפוקתיים** – השירותים המפורטים בסעיף 2 להלן שיסופקו על בסיס תכולת עבודה מוגדרת.
- 1.2.2 **שירותים משתנים** – שירותי צוות תגובה (IR) המפורטים בסעיף 3 להלן וכן השירותים המפורטים בסעיף 4 להלן שיסופקו על בסיס צורך משתנה, ולא יכללו תכולה מוגדרת מראש אלא תכולה המשתנה בהתאם לצורכי החברה. שירותים אלה יסופקו על בסיס שעות עבודה.
- 1.3 כחלק מכל סוג שירות שיוזמן (תפוקתי או משתנה), הספק יידרש לספק את כלל השירותים בהתאם לתנאים הכללים המפורטים בסעיף 5 להלן, וזאת ללא כל תשלום ו/או תמורה נוספת מעבר למפורט בהסכם ההתקשרות.
- 1.4 מובהר כי ההזמנה והביצוע של כל שירות (תפוקתי או משתנה), תבוצע על ידי החברה ועל פי דרישתה, אשר תגדיר לכל השירות את הנחיותיה ובכלל זה את היקפו ואת לוחות הזמנים למימושו). החברה רשאית להזמין שירותים מכל סוג ובהיקף שיידרש, ואף רשאית שלא להזמין שירותים מסויימים כלל.
- 1.5 השירותים יבוצעו על ידי צוות מקצועי מטעם הספק, בהתאם להוראות סעיף 6 להלן.
- 1.6 כל השירותים יסופקו הן בתחום ה- IT והן בתחום ה- OT/IOT.
- 1.7 כלל השירותים במסמך זה יבוצעו (ככל שיוזמנו על ידי החברה) לפי הנחיותיה (ככל שתהיינה) של ראשת תחום אמו"ס בנתיבי איילון ו/או מי מטעמה ו/או מי שימונה במקומה על ידי נתיבי איילון אשר גם יהיו רשאים לפקח על השירותים כאמור. למען הסר ספק מובהר בזה, כי אין בכל פעולה שתבוצע על ידי נתיבי איילון (או שלא תבוצע) כאמור, כדי לגרוע למעט מאחריותו המלאה של הקבלן על פי ההסכם ו/או הדין.
- 1.8 התמורה עבור השירותים מפורטת בסעיף 7 להסכם.
- 1.9 כל הדרישות בנספח זה רלוונטיות לכל תקופת ההתקשרות, כולל תקופת ההארכה, ככל ותהיינה כמפורט בהסכם.

## 2 שירותים תפוקתיים

### 2.1 שירותי תוכניות עבודה בתחום אבטחת המידע

- 2.1.1 הספק יידרש להגיש הצעה לתוכנית עבודה שנתית בתחום אבטחת המידע.
- 2.1.2 תוכנית העבודה המוצעת תכלול:

- 2.1.2.1 מועדים ותכולה לביצוע סקרי סיכונים.
- 2.1.2.2 המלצה לסוגי המערכות ביצוע סקרי סיכונים, בדיקות חדירות (PT), וכן תכולה ומועדים.
- 2.1.2.3 תוכנית לעדכוני גרסאות וביצוע הקשחות.
- 2.1.2.4 תוכנית לביצוע תרגילי המשכיות עסקית ושרידות.
- 2.1.2.5 תוכנית לעדכון נהלים בתחום אבטחת המידע והסייבר.
- 2.1.2.6 תוכנית הדרכות למשתמשי הקצה של החברה ולגורמים באגף מערכות מידע.
- 2.1.2.7 תוכנית בקרה על אופן השימוש והתחזוקה של מערכות המידע בשימוש החברה.
- 2.1.3 ההצעה לתוכניות תוכן בפורמטים שייקבעו על ידי החברה.
- 2.1.4 תוכנית העבודה תכלול התיחסות לנושאים הבאים – יעדים לכל משימה, לוח זמנים / מועדים למימוש, משאבים נדרשים למימוש.
- 2.1.5 ההצעה תוצג בפני הנהלת החברה וכן ייצוג בפני רגולטורים נוספים (כגון – משרד התחבורה, מערך הסייבר הלאומי ועוד). הספק יידרש לעדכן ו/או לתקן ו/או לשנות את התוכנית המוצעת בהתאם להערות שיקבל ולמען הסר ספק ללא כל תשלום ו/או תמורה נוספת.
- 2.1.6 הספק יידרש לבצע בקרה ופיקוח אחר מימוש תוכנית העבודה המאושרת. במסגרת הבקרה יידרש הספק (בין היתר) לבצע:
- 2.1.6.1 הגשת דוח רבעוני המנתח את העמידה ביעדי התוכנית (לוח זמנים ותכולות).
- 2.1.6.2 להציע הצעות לסגירת פערים לעמידה בתוכנית העבודה.
- 2.1.6.3 עדכונים מוצעים בתוכנית העבודה.
- 2.2 הכנת סקרי סיכונים**
- 2.2.1 הספק יידרש לבצע סקר סיכונים.
- 2.2.2 סקרי הסיכונים יכללו:
- 2.2.2.1 מיפוי אירועי אבטחת מידע וסייבר אפשריים (כגון חדירות כופרה, תקיפות service of Denial, חדירת קוד עיון, בחינת פרצות לחוות השרתים או ל Domain).
- 2.2.2.2 הערכות ואמצעי הגנה בפני תקיפות סייבר – הגדרת בעלי תפקיד, מערכות להתרעה, ביצוע גיבויים, שיאפשרו שיחזור נתונים שנפגעו, תהליכי תחקור והפקת לקחים.

- 2.2.2.3 נוהל מפורט (Play Book) לפעולה בעת אירוע סייבר בכל סוגי המתקפות (לרבות – Malware, Ransomware, Distributed denial of service attacks, Spam and Phishing וכיו').
- 2.2.3 סקרי הסיכונים יערכו על בסיס שיטות מקובלות בתחום זה, אשר יוצגו על ידי הספק לאישור החברה.
- 2.3 תכנון וביצוע תרגול DR
- 2.3.1 תכנון תוכנית לביצוע הגלישה הכולל תרחישים להפעלה תרחיש התרגיל.
- 2.3.2 ליווי מימוש התרגיל בהתאם לתוכנית (יבש ורטוב).
- 2.3.3 ליווי החזרה לתפקוד באתר הראשי.
- 2.3.4 הפקת לקחים.
- 2.4 ביצוע הדרכות
- 2.4.1 הספק יידרש לבצע הדרכות מעת לעת לגורמים שונים בחברה (הנהלה, משתמשי קצה, אנשי תשתיות, קבלני משנה).
- 2.4.2 תכולות ההדרכה ייקבעו על ידי החברה, בהתאם לצורך.
- 2.4.3 נושאי ההדרכה עשויים לכלול:
- 2.4.3.1 התמודדות עם סיכוני הסייבר.
- 2.4.3.2 הנחיות לפיתוח מאובטח.
- 2.4.3.3 הקשחות.
- 2.4.4 ההדרכות יבוצעו במשרדי החברה.
- 2.4.5 כל הדרכה תארך עד 4 שעות. ככל תידרש הדרכה קצרה יותר- החברה תוכל, לפי שיקול דעתה הבלעדי, לשלם לספק חלק מהתמורה להדרכה בת 4 שעות כפי שהציע הספק במכרז באופן יחסי או לשלם תמורה אשר תחושב על בסיס התעריפים השעתיים לצורך מתן השירותים המשתנים (בניכוי אחוז ההנחה המוצע על ידי הספק במסגרת המכרז).
- 2.4.6 הספק יידרש לספק לכל הדרכה מדריכים ועזרי הדרכה.
- 2.4.7 בתום ההדרכה יידרש הספק לבצע בחינה למשתתפים ולהעניק תעודות סיום למסיימים שיעמדו בדרישות ההדרכה.
- 2.5 סקירות מקצועיות בתחום אבטחת המידע
- 2.5.1 הספק יכין סקירה תקופתית בנושא כלי אבטחת המידע בשימוש החברה.
- 2.5.2 הסקירה תכלול:

- 2.5.2.1 מיפוי כלל כלי אבטחת המידע המצויים בשימוש החברה (יצרן, גרסה, ממשקים, הגדרות).
- 2.5.2.2 סקר לגבי שינויים צפויים במוצרים קיימים ברשות החברה (עדכוני גרסאות, הטלאות, שיפורים וכד').
- 2.5.2.3 התראה על end-of-Sale או end-of-support של מוצרי אבטחת מידע ברשות החברה.
- 2.5.2.4 סקר שוק לגבי חלופות למוצרים הקיימים.
- 2.5.2.5 השוואת יכולות.
- 2.5.2.6 משמעות למעבר למוצרים חליפיים, כולל אינטגרציה עם מוצרים אחרים בשימוש החברה ו אומדני עלות וניתוחי כדאיות כלכלית.
- 2.5.3 הסקירה תוגש בפורמטים שייקבעו על ידי החברה.

### 3 שירותים משתנים - צוות התגובה (INCIDENT RESPONSE)

- 3.1 הספק נדרש להגדיר צוות תגובה אשר יהיה זמין למתן שירות בקרות אירועי אבטחת מידע וסייבר, לפי הוראות סעיף זה.
- 3.2 מטרת צוות התגובה – מוכנות של צוות מקצועי לסייע לחברה בקרות אירועי סייבר בצמצום השפעת האירוע, ביצוע פעולות לסגירת הפרצות ובחזרה מהירה לשגרה.
- 3.3 השירותים מצוות התגובה עשויים בין היתר לכלול (הכל בהתאם להנחיית החברה):
- 3.3.1 זיהוי הפרצות והתקלות במערכות החברה שאותרו על ידי מוקד ה SOC של החברה ו/או של מי מטעמה או בכל דרך אחרת.
- 3.3.2 הכנת תוכנית פעולה לסגירת הפרצות וחזרה לשגרה ובקרה אחר יישומה.
- 3.3.3 תיאום ואינטגרציה של כלל הגורמים המעורבים (לרבות – הנהלת החברה, רשות הסייבר, גורמי הביטחון במשרד התחבורה, מנהלי המתקנים, קבלני מערכת וכד').
- 3.3.4 סיוע בשחזור מידע והחזרת המערכות לכשירות.
- 3.3.5 נטרול וניקוי פוגענים.
- 3.3.6 ניהול מו"מ על כופר במידת הצורך.
- 3.3.7 הכנת תוכנית לחזרת הארגון לשגרה.
- 3.3.8 איסוף ראיות פורנזיות דיגיטליות באופן תקף מקצועית וקביל משפטית במהלך האירוע.
- 3.3.9 שימור ראיות וסיוע מול חברות הביטוח לקבלת שיפוי.
- 3.3.10 הפקת לקחים.

### 3.4 דרישות מצוות התגובה

3.4.1 צוות התגובה יכיל את אנשי המקצוע אשר יעמדו לכל הפחות בדרישות המינימאליות שלהלן:

#	תפקיד	דרישות מינימאליות
1.	מומחה סייבר	ניסיון של 5 שנים לפחות בביצוע סקרי סיכונים בנושא בטחון מידע והגנה בסייבר
2.	מומחה הטמעה והדרכה	ניסיון של 5 שנים בהטמעה ובקרת יישום מדיניות בטחון מידע והגנה בסייבר
3.	יועץ אסטרטגי בתחום הסייבר	ניסיון של 5 שנים ביעוץ אסטרטגי לביטחון מידע והגנה בסייבר ללקוחות להם לפחות 500 משתמשים
4.	מנהל פרויקטים	בעל ניסיון בניהול אחראי פרויקטים בתחום מודעות לנושאי בטחון מידע והגנה בסייבר
5.	מומחה חקירות סייבר	בעל התמחות מעל 3 שנים בחקירות , FORENSICS בשניים או יותר מתוך התחומים הבאים: מחקר פורנזי, מחקר רשתות, מחקר איומים ומערכי תקיפה, מחקר מודיעין סייבר, ניסיון בחילוץ תובנות מחקריות ממידע מודיעיני - טכנולוגי, ביצוע מבדקי חדירות, טיפול ותגובה לאירועים.
6.	מומחה תשתיות WINDOWS	בעל התמחות של מעל 3 שנים במוצרי Microsoft לרבות Windows Server וגיבוי. Windows Active Directory התקני אחסון
7.	מומחה תשתיות LINUX	בעל התמחות של מעל 3 שנים במוצרי Linux, Windows לרבות Active Directory התקני אחסון וגיבוי.
8.	מומחה IOMT / OT	ניסיון של שנתיים לפחות בניטור מערכות IOMT

3.4.2 צוות התגובה יהיה זמין 24 שעות ביממה, 365 ימים בשנה.

3.4.3 פרטי צוות התגובה יוגשו על ידי הספק לאישור החברה לרבות כל המסמכים והאסמכתאות הנדרשים לצורך בחינת עמידתם בדרישות המינימאליות כאמור לעיל, עד לא יאוחר מ- 20 ימי עבודה ממועד חתימת הספק והחברה על ההסכם.

3.4.4 ככל ואחד מאנשי צוות התגובה שאושרו על ידי נתיבי איילון לא יהיה זמין למשך יותר מ 7 ימי עבודה - יידרש הספק להעמיד מחליף ראוי, בעומד בכשירות לתפקיד הרלוונטי. אין באמור להוות הסכמת החברה שלא לפעול כאמור בסעיף 3.4.2 לעיל.

3.4.5 כל חבר בצוות התגובה נדרש להגיע לאתרי החברה לצרכי ריענון שוטף לפחות יום עבודה אחד ברבעון קלנדרי (יום מלא או 2 חצאי יום). תכולת הריענון תיקבע על ידי החברה ותכלול – הכרות עם מערכות החברה, נכסי מידע ואמצעי אבטחה.

3.4.6 החברה תקבע את המועד לביצוע הריענון ואת תכולת העבודה שתידרש מצוות התגובה במסגרת זו..

### 3.5 הפעלת צוות התגובה

3.5.1 הודעה על הפעלת צוות התגובה תימסר על ידי החברה לאיש הקשר מטעם הספק. הפעלת צוות התגובה כאמור תבוצע במייל או בטלפון והיא תכלול בין היתר את הרכב צוות התגובה שיופעל.

3.5.2 בהודעת ההפעלה ייכלל מידע שיהיה בידי החברה במועד ההפעלה, לדוגמה:

3.5.2.1 תיאור הבעיה.

3.5.2.2 השירות הנדרש.

3.5.2.3 משך חזוי להפעלת השירות הנדרש.

3.5.3 הפעלת צוות התגובה (או אי הפעלה) וכן הרכב הצוות שיופעל, יהיו בהתאם להחלטת החברה בלבד, לפי שיקול דעתה. יובהר כי החברה איננה מחויבת להפעיל את כל הצוות שנמצא בכוננות, ותוכל להפעילו באופן חלקי.

3.5.4 צוות התגובה יופעל בהתאם להנחיות החברה.

3.5.5 הספק יידרש להפעיל את צוות התגובה בהתאם ליעד הזמינות להלן:

3.5.5.1 נדרשת תגובה טלפונית תוך שעה, לרבות התחברות מרחוק במקרה הצורך.

3.5.5.2 החברה תוכל לדרוש את הגעת צוות התגובה לאתר ובמקרה כאמור תחילת הטיפול יהיה תוך 4 שעות (זאת בכל שעה או יום שיידרש).

3.5.5.3 במקרה של הגעת צוות התגובה לאתר כאמור - החברה תוכל לדרוש המשך שהות באתר באופן רציף (24 שעות ברציפות, מספר ימים ברצף). במקרה כזה יידרש הספק לספק חברי צוות תגובה חליפיים לחברי צוות התגובה (שפרטיהם יובאו לאישור אצל החברה בהקדם האפשרי), כך שניתן יהיה לספק שירות רצוף. הספק נדרש לספק לצוות התגובה את כל הציוד והאמצעים הנדרשים (לרבות – אמצעי תחבורה להגעה לאתרי החברה, מזון, מים, חשמל, מחשבים ניידים עם תוכנות מתאימות וכו').

3.5.6 בתום הפעלת צוות התגובה – יידרש הספק להגיש דוח סופי הכולל את פירוט הפעולות שבוצעו, הצעה ללקחים.

#### 4 שירותים משתנים – שירותים נוספים

4.1 החברה תוכל לבקש מהספק לבצע שירותים משתנים נוספים, בהתאם לצורך ולשיקול דעתה הבלעדי כמפורט בסעיף 4 זה.

4.2 שירותים בתחום פרויקטים טכנולוגיים:

4.2.1 כתיבת פרוגרמות, הנחיות ומסמכי צורך בתחום אבטחת המידע.

4.2.2 כתיבת דרישות לפרויקטים בתחום אבטחת המידע.

4.2.3 הגדרת ארכיטקטורות לנושא אבטחת המידע בפרויקטים.

4.2.4 בדיקת מענים למכרזים הכוללים דרישות בתחום אבטחת המידע והסייבר.

4.2.5 בקרה אחר הקמת מערכות בתחום אבטחת המידע.

4.2.6 בחינת התאמה של העברת מערכות, אפליקציות ו/או מידע לענן.

4.2.7 כתיבת תרחישים לבדיקת מערכות במהלך בדיקות מסירה / קבלה.

4.2.8 השתתפות בשלב בדיקות קבלה בתחום אבטחת המידע.

4.2.9 ליווי הטמעות של מערכות טכנולוגיות בהתאם להנחיות אבטחת המידע.

4.2.10 כתיבת דוחות מסכמים לפני מתן אישור לעלייה לאוויר.

4.3 שירותים שוטפים בתחום אבטחת המידע:

4.3.1 כתיבת מסמכים ונהלים כמפורט בסעיף 4.4 להלן.

4.3.2 הנחיות בנושא הגדרת FW.

4.3.3 בדיקות פיתוח קוד.

4.3.4 ניתוח מידע המתקבל ממוקד ה SOC המופעל על ידי החברה ו/או מי מטעמה.

4.3.5 ליווי צוות התגובה שיופעל על ידי הספק.

4.3.6 עריכת שאלונים ומבחני הסמכה.

4.3.7 בקרה ופיקוח על תחזוקה וניהול פעילות תקינה של כלל אמצעי האבטחה במערכות המידע בשימוש החברה בקרב המשתמשים של החברה. הבקרה תבוצע בקרב הספקים המספקים שירותים למערכות מידע טכנולוגיות בשימוש החברה.

4.3.8 ביצוע תרגילי אבטחת מידע לרבות תכנון מפורט של ביצוע התרגיל, תיאום ביצוע התרגילים, סיכום תוצאות התרגיל והקפת לקחים.

4.3.9 ביצוע תרגילי Phishing.



- 4.3.10 ביצעו בדיקות חדירה מסוים שונים.
  - 4.3.11 השתתפות בתרגילי הנהלה.
  - 4.3.12 ביצוע ביקורות אבטחת מידע למשתמשי הקצה.
  - 4.3.13 בקרות שרשרת אספקה.
  - 4.3.14 בחינת ליקויים במערך אבטחת המידע, זיהוי Single points of failure.
  - 4.3.15 חקירת אירועי אבטחת מידע הכוללים: בחינת היקף הנזק שנגרם, תכנון שיקום הנזקים, ניתוח שיטות הפעולה באירוע, המלצה ללקחים.
- 4.4 כתיבת מסמכי מדיניות ונהלים**
- 4.4.1 מנהל הפעילות מטעם הספק יידרש לעדכן את נהלי אבטחת המידע של החברה.
  - 4.4.2 הנהלים יכללו:
    - 4.4.2.1 דרישות מקצועיות לרכש והפעלת מערכות טכנולוגיות.
    - 4.4.2.2 דרישות להעסקת כ"א בחברה.
    - 4.4.2.3 נוהל התמודדות עם אירועי סייבר.
    - 4.4.2.4 נוהל התמודדות במצב חירום בהיבטי אבטחת המידע.
    - 4.4.2.5 נוהל תרגול נדרש לבחינת תפקוד החברה בעת אירוע סייבר (יבש ורטוב).
    - 4.4.2.6 הנחיות לעמידה בתקנים מחייבים (GDPR, 27001 וכד).
  - 4.4.3 העדכון יבוצע על בסיס:
    - 4.4.3.1 מועדי העדכון שנקבעו בתוכנית העבודה המאושרת.
    - 4.4.3.2 עדכון בהנחיות הפנימיות של החברה.
    - 4.4.3.3 הנחיות של רגולטורים.
    - 4.4.3.4 לקחים ומידע מחברות העוסקות בתחומים דומים בארץ ובעולם.
    - 4.4.3.5 צורך הנגזר ממידע כללי ברשות הספק.
  - 4.4.4 הנהלים ייכתבו בפורמטים שייקבעו על ידי החברה.
  - 4.4.5 הספק יידרש להכין לחברה לומדות ועזרי הדרכה להדרכות על בסיס הנהלים.
  - 4.4.6 הספק יידרש לקבל את אישור הגורמים הרלוונטיים לנוהל המעודכן (לרבות רגולטורים ומנחים מקצועיים בחברה).
- 4.5 שירותי דיונים וייצוג מול גורמי רגולציה, כדוגמת הבאים:
- 4.5.1 השתתפות בדיונים העוסקים בתחום אבטחת המידע בחברה ומול גורמי רגולציה.

- 4.5.2 הכנת מצעים לדיונים, מסמכי עמדה וחוות דעת מקצועיות בהתאם לצורך.
- 4.5.3 ייצוג החברה מול גורמי הרגולציה, ליווי גורמי הרגולציה בעת עריכת ביקורות בחברה ובקרב גורמים מטעמה.
- 4.5.4 סיכומי דיון, גזירת הנחיות ומעקב אחר יישומן.
- 4.6 שירותי בקורת על מאגרים המנוהלים, כדוגמת הבאים :
- 4.6.1 הגדרת דרישות
- 4.6.2 ביצוע סקרים לעמידה בדרישות הדין.
- 4.6.3 יעוץ וליווי לפרויקטים בהם נדרש להקים ולנהל מאגרי נתונים.
- 4.6.4 ייצוג למול הרשות להגנת הפרטיות.

## 5 הוראות כלליות לביצוע השירותים

- 5.1 כלל התכולות שפורטו לעיל הינן תכולות כלליות ומינימאליות, ועל הספק לבצע את השירותים בהתאם לסטנדרטים מקובלים ובהתאם למסמך המתודולוגיה לשירותים התפוקתיים שהגיש במסגרת הצעתו למכרז.
- 5.2 הספק יבצע את השירותים רק בהתאם להזמנת עבודה בכתב שתופק על ידי החברה.
- 5.3 יובהר כי החברה איננה מחויבת להזמין את השירותים (התפוקתיים או המשתנים או אחרים מכל סוג שהוא) מסוג או בהיקף כלשהו ואף רשאית שלא להזמין כלל, והכל בהתאם לשיקול דעתה.
- 5.4 החברה תחליט על תדירות כל שירות.
- 5.5 הספק מחוייב להיות ערוך לספק כל שירות כמכלול, בהתאם לדרישות המפורטות במסמך זה.
- 5.6 על הספק להתחיל את ביצוע השירותים התפוקתיים בהתראה של עד 5 ימי עבודה מרגע הזמנתם על ידי החברה (ככל שיוזמנו).
- 5.7 עם תחילת כל שירות, הספק יידרש להעביר לאישור החברה, תוכנית מפורטת לביצוע השירות. התוכנית שתוגש תכלול (בין השאר) :
- 5.7.1 תוצרים צפויים.
- 5.7.2 פירוט מלא של הפעולות שיבוצעו על ידי הספק במסגרת השירות.
- 5.7.3 לוח זמנים מפורט ואבני דרך לביצוע השירותים.
- 5.7.4 פירוט הצוות ושאר האמצעים שנדרשים עבורו כדי לספק את השירות.
- 5.7.5 פירוט תכולת הדוח הסופי שיוגש לחברה ופורמט ההגשה.

## 6 הצוות המקצועי

- 6.1 כללי
- 6.1.1 הספק יישא באחריות המלאה והבלעדית לכך שבכל עת במהלך תקופת ההתקשרות יוקצו לטובת ביצוע השירותים, בעלי מקצוע בעלי הכשרה מתאימה, ובכל היקף שיידרש לצורך ביצוע והשלמת השירותים בהתאם לנדרש ובמועד, בהתאם לדרישות ההסכם.
- 6.1.2 הספק יקבע את הרכב אנשי המקצוע שיבצעו את השירותים התפוקתיים, באופן שיביא לכך שהספק יעמוד בדרישות מסמכי ההסכם לרבות מסמך זה ובהנחיות החברה.
- 6.1.3 עבור שירותים המשתנים – יידרש הספק לגייס אנשי מקצוע בהתאם למהות השירות. יובהר כי אנשי המקצוע הנוספים יוכלו להיות קבלני משנה של הספק.
- 6.1.4 יובהר כי למעט ביחס למנהל הפעילות אין במכרז דרישה להקפי משרה מסוימים, אלא דרישות לזמינות בלבד. היקף העסקתם של אנשי המקצוע בצוות המקצועי ייקבע על ידי הספק כדי לעמוד בדרישות החברה.
- 6.2 מנהל הפעילות
- 6.2.1 מנהל הפעילות אשר הוצג על ידי הספק במסגרת הצעתו למכרז, יידרש לנהל ולרכז את כל השירותים מטעם הספק.
- 6.2.2 במסגרת זו יידרש מנהל השירותים, בין היתר, כדלקמן:
- 6.2.2.1 לייצג את הספק בפני החברה.
- 6.2.2.2 לנהל את הצוות המקצועי מטעם הספק
- 6.2.2.3 לפקח ולבקר את פעילות כלל הצוות המקצועי מטעם החברה.
- 6.2.2.4 להשתתף בכל דיון שיוזמן על ידי החברה הקשור לשירותים.
- 6.2.3 מנהל הפעילות יהיה זמין לפעילות בשעות העבודה הרגילות (ימים א'-ה' בין השעות 08:00-17:00) (להלן: "שעות העבודה הרגילות") ובכלל זה יגיע למשרדי נתיבי איילון ככל שיונחה לכך על ידי נתיבי איילון, והכל על פי הנחיות נתיבי איילון לפי שיקול דעתה הבלעדי. לצורך הערכות המציעים להגשת הצעתם למכרז, ומבלי שהדבר יהווה מצג ו/או התחייבות של נתיבי איילון מובהר בזאת כי ממוצע השעות החודשי של היועץ שהעניק לנתיבי איילון שירותים בתחום בשנה שחלפה היה 160 שעות חודשיות.
- 6.3 גיוס אנשי המקצוע נוספים
- 6.3.1 החברה תהיה רשאית לדרוש מהספק כי השירותים המשתנים יבוצעו על ידי אנשי מקצוע בעלי ניסיון / הסמכות מסוימות. לצורך כך, החברה תגדיר דרישות מקצועיות ביחס לשירותים המקצועיים הנוספים יוזמנו על ידה.
- 6.3.2 הספק נדרש להציג לאישור החברה את אנשי המקצוע בהתאם להנחיותיה ולקבלו עבור כל מטלה, לפני ביצועה בפועל.

- 6.3.3 הספק מתחייב להמציא לידי החברה את כל המסמכים הנדרשים לצורך הוכחת עמידת אנשי המקצוע בדרישות הרלוונטיות.
- 6.3.4 אנשי המקצוע יוצגו לאישור החברה תוך 15 ימי עבודה ממועד קבלת הדרישה לשירות נוסף מסויים.
- 6.3.5 מבלי לגרוע מכל זכות של החברה, היא תהיה רשאית לבחון ו/או לראיין את המועמדים לתפקידי אנשי המקצוע וכן תוכל לסרב לקבל שירותים מידיהם ו/או באמצעותם, הכל לפי שיקול דעתה הבלעדי של החברה.
- 6.3.6 הספק יידרש להציב את אנשי המקצוע שיאושרו על ידי החברה בתפקידם תוך עד 14 ימי עבודה לאחר קבלת אישור החברה.
- 6.3.7 כל חברי הצוות המקצועי שיאושרו על ידי החברה, יהיו זמינים למתן שירותים לחברה בתוך 48 שעות מהזמנת השירות על ידי החברה, במהלך שעות העבודה הרגילות (כהגדרתן לעיל).
- 6.4 שינוי והחלפת אנשי מקצוע בצוות המקצועי :
- 6.4.1 החברה תוכל לדרוש מהספק כי יחליף אחד או יותר מבעלי המקצוע הנכללים בצוות המקצועי בכל עת ומכל סיבה סבירה, והספק ימנה איש מקצוע חלופי תוך עד 14 ימי עבודה, בהתאם לתהליך שתואר לעיל.
- 6.4.2 במקרה שחבר בצוות המקצועי יחליט על סיום עבודתו אצל הספק - יודיע הספק על כך לחברה מיד עם היוודע לו הדבר.
- 6.4.3 הספק יתחייב לכך שהחלפת נציג בצוות המקצועי מכל סיבה שהיא לא תפגע בהתחייבויותיו על-פי מכרז זה.
- 6.4.4 החלפת חבר בצוות המקצועי תאושר רק לאחר מינוי מחליף. המחליף יהיה בעל כישורים שאינם נופלים מחבר הצוות המקצועי המוחלף, בהתאם לשיקול דעתו של נציג החברה