מדינת ישראל - משרד התחבורה

חירום, ביטחון מידע וסייבר

מכרז 11/2026

לאפיון, הקמה והתפעול של מרכז ניטור ותגובה סייבר במגזר התחבורה (TSOC)

(גרסה 1)

את מסמכי המכרז ניתן למצוא באתר האינטרנט של מינהל הרכש הממשלתי בכתובת:
www.mr.gov.il תחת הכותרת – מכרז 11/2026 – לאפיון, הקמה והתפעול של מרכז ניטור ותגובה סייבר במגזר התחבורה (TSOC)

1. הקדמה

1.1. משרד התחבורה **("המזמין")**, מפרסם בזאת מכרז 11/2026 לאפיון, הקמה והתפעול של מרכז ניטור ותגובה סייבר במגזר התחבורה (TSOC) **("המכרז")**.

1.2. אגף החירום, הביטחון, המידע והסייבר (להלן: ***"האגף"***) במשרד התחבורה מפרסם בזאת מכרז לאספקת שרותי אפיון, תכנון, יישום, הטמעה, הקמת ותפעול מרכז ניטור אבטחת סייבר (להלן ה- (TSOC) על תשתיות וחברות חיוניות במגזר התחבורה (להלן גם- המגזר). יודגש שאין מדובר בSOC עבור רשתות משרד התחבורה אלא עבור משרד התחבורה לניטור מגזר התחבורה והחברות/הארגונים המשתייכים אליו.

1.3. הקמת מרכז ניטור אבטחת סייבר (TSOC) למשרד נועדה לתכלל את כלל הנושאים, הצרכים והמערכות הנדרשים לשם איסוף הנתונים, מחקרם, ניתוחם, שיתופם והצגתם במקום מרכזי אחוד, לצורך ראית תמונת מצב האבטחה בסייבר וחוסן המגזר בכללותו, לבקר את תמונת המצב, לשתף במידע ובמידת הנדרש להעביר הנחיות, להתריע כנגד התקפות ואף לסייע בחוסן הגורמים המנוטרים (ג"מים) להתמודד אל מול אירועי סייבר תוך אחזקת תמונת איומים טכנולוגיים רציפה, עדכנית ורלוונטית.

הזוכה שיוכרז במכרז יחתום על הסכם התקשרות (מצ"ב כפרק ד') עם המזמין לתקופה של 24 חודשים **("תקופת ההתקשרות")**, כאשר למזמין הזכות להאריך את תקופת ההתקשרות בתקופות נוספות, ועד ל - 48 חודשים נוספים (6 שנים מצטברות).

1.4. מסמכי המכרז מחולקים לפרקים, כמפורט להלן:

1.4.1. **פרק א'** – ההליך המכרזי.

1.4.2. **פרק ב'** – חוברת ההצעה, אשר תוגש על ידי מציע המתמודד במכרז.

1.4.3. **פרק ג'** – תכולת ההתקשרות עם הספק הזוכה.

1.4.4. **פרק ד'** – הסכם ההתקשרות עם הזוכה במכרז.

<u>המועד האחרון להגשת הצעות במכרז הוא בתאריך 13/08/2026 בשעה 14:00</u>

2. תוכן עניינים

פרק א׳- הליך המכרז

3. עקרונות המכרז

מכרז זה הוא מכרז פומבי הנערך בהתאם לחוק חובת המכרזים, התשנ"ב-1992 (**"חוק חובת המכרזים"**) ותקנותיו, ובכלל זה תקנות חובת המכרזים, התשנ"ג-1993 (**"תקנות חובת המכרזים**.("

3.1. במסגרת הליך המכרז, הצעות אשר יוגשו במכרז יידרשו לעמוד בתנאי הסף להשתתפות במכרז המפורטים להלן. ההצעות אשר עמדו בתנאי הסף של המכרז, ידורגו בהתאם לאמות המידה המפורטות במכרז.

3.2. בתום הליך המכרז, המזמין יכריז על המדורג ראשון כזוכה במכרז ויחתום עימו על הסכם התקשרות, הכל כמפורט להלן.

המכרז יתנהל בהתאם לדין, ולפי כללי המכרז המפורטים במסמכי המכרז.

תכולת המכרז כוללת את המרכיבים הבאים:

- הקמה פיסית של מרכז במסגרת תשתית קיימת ,לרבות ריהוט ואיבזור
- הקמת המעטפת הטכנולוגית לביצוע משימות המרכז
- גיבוש תפיסת הפעלה ותפיסת תיפעול של המרכז ,לרבות גם במצבי חירום ומשבר והטמעתה
- איוש בעלי תפקידים מקצועיים בהתאם לתפיסה
- תפעול המרכז ,לרבות גם במצבי חירום ומשבר

4. תנאים להשתתפות במכרז

4.1. **תנאי סף להשתתפות במכרז**

4.1.1. רשאי להשתתף במכרז מציע אשר עומד, במועד האחרון להגשת ההצעות, בתנאי הסף להשתתפות במכרז המנויים להלן.

4.1.2. הוכחת העמידה בתנאי הסף המנויים להלן, תתבצע בהתאם להוראות חוברת ההצעה (**פרק ב**).

4.2. **תנאי סף מנהליים:**

4.2.1. אם חלה על המציע חובת רישום, על פי דין, בישראל, עליו להיות רשום כדין.

4.2.2. המציע עומד בדרישות חוק עסקאות גופים ציבוריים, התשל"ו- 1976 (**"חוק עסקאות גופים ציבוריים"**).

4.2.3. כלל המוצרים והשירותים המוצעים על ידי המציע עומדים בדרישות הרישוי והתקנים הנדרשים על פי דין לצורך אספקתם, אם ישנם.

4.2.4. **מידע פלילי רלוונטי** –

4.2.4.1. למציע או נושאי משרה רלוונטיים אצל המציע אין מידע פלילי רלוונטי למכרז במרשם הפלילי או המרשם המשטרתי (כהגדרתם בחוק המידע הפלילי ותקנת השבים, התשע"ט-2019) בעבירות, אחת או יותר, לפי אחד החוקים הבאים:

4.2.4.2. רשימת המידע הפלילי:

4.2.4.2.1. עבירות גניבה – סעיפים 290 עד 297 לחוק העונשין, התשל"ז-1977 (להלן: "חוק העונשין")

4.2.4.2.2. עבירות מרמה – סעיפים 414 עד 438 לחוק העונשין

4.3. **תנאי סף מקצועיים:**

4.3.1. **המציע עומד בתנאים המפורטים להלן:**

4.3.1.1. **נסיון – שנות נסיון** –

4.3.1.1.1. למציע ניסיון מוכח של 4 שנים בין השנים 2021-2025:

4.3.1.1.2. למציע ניסיון מוכח של ארבע (4) שנים לפחות בהקמת ותפעול מערכות מחשוב ומערכות אבטחת מידע וסייבר הכוללות מספר מעגלי אבטחת מידע לוגיים וטכנולוגיים, מערכות ניטור אבטחה בתצורת On-Prem וענן, הקמת פורטל ארגוני מגזרי מאובטח או פורטל ממשלתי או צבאי.

4.3.1.1.3. נסיון מוכח בהקמה של מרכז ניטור רב ארגוני מאובטח לרבות ממשלתי או צבאי.

4.3.1.1.4. למציע יש ניסיון מוכח של ארבע (4) שנים לפחות בתכנון והקמת פרויקטים מורכבים וחדשניים המשלבים גם מאמצים של מחקר ופיתוח בתחום הסייבר.

4.3.1.1.5. המציע העסיק במהלך השנים 2022-2025 צוות עובדים מקצועי בתחום הנדרש במכרז הכולל עשרה (10) עובדים מקצועיים לפחות, במקצועות המפורטים מטה בצוות ההקמה ובצוות ה-TSOC ולכל הפחות עובד אחד בעל ידע ונסיון רלוונטי מכל תפקיד המוצג.

4.3.1.2. **נסיון מקצועי, היקף פעילות** –

4.3.1.2.1. המציע הינו בעל מחזור פעילות שנתי בתחום הקמת והפעלת מרכזי ניטור רב ארגוניים ו/או בכלים המוצעים בהצעתו בהיקף שנתי מינימאלי של 6 מיליון ₪ בכל אחת מהשנים 2022-2025. לצורך הוכחת סעיף זה על המציע לצרף להצעתו דו"חות כספיים מבוקרים או אישור רואה חשבון מבקר המציין את היקפי המחזור של המציע בכל אחת מהשנים האמורות, בהיקף כספי של 6,000,000 ₪ לפחות.

4.3.1.3. **צוות הקמה** –

4.3.1.3.1. **<u>צוות הקמה</u>** - הצוות מיומן ומנוסה שיהיה אחראי על השלבים א'- וב' כמפורטים באבני הדרך לביצוע המכרז. הצוות יפעל בשיתוף עם נציג המשרד ובהכוונתו למימוש השלבים ולחפיפה מסודרת והעברת הידע לצוות ההפעלה המבצעית.

4.3.1.3.2. על המציע להציג במסגרת הצעתו את נותני השירותים מטעמו אשר יעמדו בתנאי הסף המקצועיים כמפורט להלן:

4.3.1.3.3. **<u>(א) מנהל הפרויקט</u>**

4.3.1.3.3.1. מנהל הפרויקט הינו בעל תואר ראשון לפחות במדעי המחשב או מערכות מידע או הנדסה ממוסד אקדמאי מוכר על ידי המל"ג. לצורך הוכחת סעיף זה על המציע לצרף את תעודות ההשכלה של מנהל הפרויקט.

4.3.1.3.3.2. מנהל הפרויקט הועסק על ידי המציע במהלך תקופה של שלוש (3) השנים האחרונות לפחות שקדמו למועד האחרון להגשת הצעות במכרז זה.

4.3.1.3.3.3. מנהל הפרויקט הינו בעל ניסיון מוכח בניהול של לפחות שלושה (3) פרויקטים בתחום הנדרש במכרז זה במהלך 4 השנים שקדמו למועד האחרון להגשת הצעות בהיקף כספי מינימאלי של מיליון ₪ לכל פרויקט, ומספר משתמשים מינימאלי של 20 משתמשים לכל פרויקט. מנהל הפרויקט ישמש כאיש הקשר של המציע עם המשרד ויהיה אחראי על הנושאים המקצועיים ועל הנושאים המינהליים אל מול המשרד.

4.3.1.3.4. **<u>(ב) ארכיטקט מערכות</u>**

4.3.1.3.4.1. ביצע תפקיד ארכיטקט מערכות תשתית ומערכות אבטחת מידע וסייבר במשך 5 שנים לפחות.

4.3.1.3.4.2. בעל ידע מעמיק ומוכח בתשתיות טכנולוגיות, אבטחת מידע והגנת סייבר.

4.3.1.3.4.3. בעל הסמכה בתחום תשתיות טכנולוגיות ואבטחת מידע והגנת סייבר.

4.3.1.3.5. **<u>(ג) מנתח מערכות</u>**

4.3.1.3.5.1. כ"א מנוסה בניתוח מערכות המועסק על ידי המציע במהלך תקופה של שלוש (3) השנים האחרונות לפחות שקדמו למועד האחרון להגשת הצעות במכרז זה.

4.3.1.3.5.2. כ"א מנתח המערכות הינו בעל ניסיון מוכח בהכנת אפיון מפורט מהסוג הנדרש במכרז זה שבוצע בשלושה (3) פרויקטים לפחות בהיקף מינימאלי של מיליון ₪ לכל פרויקט, וזאת במהלך שלוש (3) השנים שקדמו להגשת ההצעה.

4.3.1.3.6. **<u>(ד) אחראי תפעול והטמעה</u>**

4.3.1.3.6.1. מומחה בהקמה, הטמעה ותפעול מערכות ניטור SIEM בעל נסיון של 5 שנים במערכות SIEM מובילות בקטגוריה.

4.3.1.3.6.2. - לפחות 5 שנות ניסיון בהטמעת מערכות אבטחת מידע / IT בארגונים גדולים.

4.3.1.3.6.3. - ניסיון בעבודה עם מערכות SOC קריטיות, כולל:

4.3.1.3.6.4. - SIEM (Security Information and Event Management) SPLUNK, QRadar, Sentinel, ArcSight וכו'.

4.3.1.3.6.5. - SOAR (Security Orchestration, Automation, and Response) Phantom, XSOAR, Swimlane וכו'.

4.3.1.3.6.6. מערכות ניהול קריאות Ticketing Systems ServiceNow, Jira, BMC Remedy וכו'.

4.3.1.3.6.7. Data Lake / Big Data Platforms Elastic Stack, Hadoop, Apache Spark, AWS S3. -

4.3.1.3.6.8. MFT (Managed File Transfer) פתרונות להעברת קבצים מאובטחת.

4.3.1.3.6.9. Workflow & Automation תהליכי אוטומציה וניהול משימות ב-SOC.

4.3.1.3.6.10. ניסיון בהתקנה, קונפיגורציה ואינטגרציה של מערכות אלו בארגונים גדולים.

4.3.1.3.6.11. ניסיון בעבודה עם API אינטגרציות, Webhooks ו-Scripting (Python, PowerShell, Bash).

4.3.1.3.6.12. ניסיון מוכח בניהול והגדרת חוקי אבטחה ב-Firewalls, IDS/IPS, WAF, DLP, EDR/XDR.

4.3.1.3.6.13. עבודה והטמעה של כלי להגנת ענן של ספק ענן מוביל (AWS,GCP,)

4.3.1.3.7. על המציע להוכיח את ניסיונם של נותני השירותים המוצעים מטעמו באמצעות מסמכים שיפרטו את הניסיון הרלוונטי לפי שנים. ביחס לכל אחד מנותני השירותים מטעמו, יצרף המציע גם את המסמכים הבאים:

4.3.1.3.7.1. קורות חיים של כ"א מנותני השירותים

4.3.1.3.7.2. תעודות המעידות על השכלה של כ"א מנותני השירותים

4.3.1.3.7.3. אסמכתאות מתאימות המעידות על ניסיון רלוונטי וותק של כ"א מנותני השירותים

4.3.1.3.7.4. רשימה מסודרת בטבלה של פרויקטים/עבודות קודמות וניסיון רלוונטי של כ"א מנותני השירותים בצירוף תיאור העבודה, מועד ביצועה, רשימת ממליצים ואנשי קשר של גורמים ולקוחות עבורם בוצעו עבודות בצירוף פירוט דרכי ההתקשרות עמם, כמפורט להלן.

4.3.1.3.8. יובהר כי המשרד רשאי לפנות לאנשי קשר/לקוחות מהרשימה הנ"ל או ללקוחות אחרים על בסיס מידע קיים או העולה מן ההצעה או מבדיקתה על מנת להתרשם ממידת שביעות הרצון של לקוחות אלו מהשירותים שסופקו להם ע"י נותן השירותים הרלבנטי.

4.3.1.3.9. במידת האפשר, ולצורך הוכחת עמידת נותני השירותים בתנאי הסף ובדרישות הנוספות, יש לצרף דוגמאות לעבודות רלוונטיות שבוצעו על ידי מי מנותני השירותים.

4.3.1.3.10. ההחלטה האם המציע עומד בדרישת הניסיון וההשכלה, ובכלל זה ההחלטה האם הניסיון שעליו הצביע המציע הוא ניסיון בהתאם לדרישות או האם ההשכלה הינה רלוונטית לשירותים נשוא מכרז זה, נתונה לשיקול דעתה של ועדת המכרזים.

4.3.2. **המוצרים המוצעים מקיימים את הדרישות הבאות:**

4.3.2.1. סביבת מרכז הניטור תוקם באזור ישראל במסגרת ענן הנימבוס ב- AWS או ב- GCP. לטובת העניין המציע יוגדר כספק צד ג' למכרז נימבוס ויהיה זכאי להתקשרות ישירה בתנאים נימבוס אל מול ספקי שירות הענן AWS או GCP.

4.3.2.2. **התבססות על מוצרים מובילים** - כלל המערכות ומוצרי ה SaaS המסופקות במענה למרכז ניטור סייבר תחבורה - כולם יהיו מהקטגוריות המובילות (ללא מוצרים נישתיים - niche players) על בסיס מדד Gartner (באחד מ-

3 הדו"חות האחרונים) ויספקו את שרותיהם באזור המשילות הישראלי בהתאם להגדרות בפרויקט נימבוס.

4.3.2.3. **עקרון תכנון ענן - FinOps** – המענה המוצע מתבקש להיות בתצורת מבוססת ענן - נדרש לבצע תכנון מקיף של המענה תוך התחשבות בכלכלת ענן יעילה בהתאם לעקרונות FinOps תוך ביצוע בקרה, אכיפה, משילות והתייעלות קבועה ומתמשכת ליצירת אפקטיביות אופטימלית של ההצעה בהיבט הכלכלי תוך הערכת צפי עלויות עבור כל שלבי הפרויקט. הפתרון הטכנולוגי ייקח חשבון את עקרונות FINOPS "כלכלת ענן חכמה" ותבוסס על עקרון ה-OPEX תוך יצירת ניהול משאבים הדוק עבור כל הפרויקט ותתי המרכיבים במטרה ליעילות כלכלית מקסימלית ושקיפות מלאה וקלה למקבלי ההחלטות - יוצג תחשיב עלויות מוערך על בסיס ההצעה לתקופת ההקמה, לתקופת ההפעלה ולתקופת האופציה.

5. ניקוד ההצעות

5.1. אמות מידה לניקוד הצעות במכרז

5.1.1. הניקוד של כל הצעה במכרז יהיה בהתאם לאמות המידה הבאות:

5.1.1.1. איכות – 70%;

5.1.1.2. מחיר – 30%.

5.2. מדדי איכות

5.2.1. הערכת איכות ההצעות תיעשה לפי המשקלות הבאים:

# מס'	משקל	תיאור תנאי	המפתח לחישוב
1	50%	היישום המוצע	איכות המענה על בסיס האפיון הראשוני המפורט והמלא שיגיש המציע כחלק מהמענה על בסיס הדרישות המקצועיות (פרק ג' - חלק 1) בדגש על: (1) 30% - מערכת "על" - איכות פתרון הניטור (SIEM, קולקטור וכד') עפ"י הקטגוריות המובילות של גרטנר (ללא מוצרים נישתיים. בפרט אופן איסוף המידע, טיובו, דיוקו ואופן ביצוע הקורלציות לאירועים והצגתם כחלק מתמונת המצב המגזרית. (2) 10% פתרון שו"ב מרכזי - על כלל מרכיביו - אפקטיביות ותכלול כלל המרכיבים המאפשר ניהול הטיפול באירועי סייבר, תיעוד האירועים, יכולת אחזור אירועי עבר קשורים (קורלציות), הפקת דוחות, יצוא דוחות, תיעוד פעולות, ניהול משמרות, כלי ניהול ומודל תומך החלטה. מאגר הסייבר המרכזי ומערכת מחקר, ניתוח והעשרת מידע - תשתית מידע אחודה, מבוססת טכנולוגיית BIG DATA \DATA LAKE המאפשרת לאגור את כלל המידע לטווח קצר ולטווח ארוך. תשתית המאפשרת לבצע מחקר וניתוח של אירועי סייבר מעל תשתית מאגר הסייבר המרכזי ומשתמשת ככלי ניהול, ניתוח והעשרת המידע מערכות תפעול תומכות המערכות SOAR ו- Manage File Transfer ומערכות תומכות נוספות לתפקוד המרכז TSOC. (3) 10% תשתיות אבטחה למרכז - מתן מענה מקיף ברמת מערכות אבטחה למרכז הסייבר אשר יספקו הגנה ואבטחה היקפית כמענה לאבטחת מרכז ה TSOC.
2	20%	טכנולוגיה	איכות המענה בהתאם לאפיון הראשוני שיוגש על ידי המציע כחלק מהמענה על בסיס הדרישות הטכנולוגיות (פרק ג' - חלק 1) בהיבט: (1) 10% - ארכיטקטורה - ארכיטקטורה מבוססת ענן משלב פתרונות SaaS\IaaS גמישה לשינויים, מבוזרת, וירטואלית ,עדכנית ושרידה הכוללת כלי ניהול, ניטור ובקרה מרכזיים, מאפשרת תחזוקה, שדרוגים ועדכונים ללא פגיעה בשרות ובזמני תגובה מהירים, ניהול גרסת מערכת, ניהול

# מס׳	משקל	תיאור תנאי	המפתח לחישוב
			גרסאות ועדכונים, שרידות וזמינות מרבית ותכנון FinOps. (2) 5% - חומרה - ציוד היקפי, תחנות קצה, STORAGE, מערכת גיבוי, התקני תקשורת ואבטחת מידע, הבטחת ביצועים ושרידות וגיבוי של מקסימלית. מפרטים טכניים של ציודים וכתב הכמויות. (3) 5% - תשתיות תוכנה ורישוי - מערכות הפעלה, תוכנת קצה, אפליקציות, סביבת בדיקות, סביבת פיתוח מאובטחת, ניהול גרסאות ותצורה. תחזוקה, שדרוגים ועדכונים על בסיס שנתי, תוכנות גיבוי, ממשקים מאובטחים לכניסה מרחוק רישוי תוכנות ותוכנות צד שלישי וכו׳.
3	30%	יכולת מימוש	(1) 10% ניסיון המציע בפרויקטים דומים. (2) 10% התרשמות כללית והמלצות. (3) 4% מנהל הפרויקט וצוות הפרויקט, לפי: • הכשרה אקדמאית • הסמכה בתחום ניהול פרויקטים PMP, MPM & CIPM • שנות ניסיון מוכח בדגש על פרויקטים גדולים בעולם טכנולוגיות אבטחת המידע והסייבר ובעולם התוכן הייעודי ל SOC עבור מגזר התחבורה • משך עבודה בהתאם לתנאי הסף המקצועיים. (4) 2% תכנית עבודה ולוח זמנים (5) 4% מתודולוגיה ותפיסת הפעלה למרכז TSOC הכוללת אנשים, טכנולוגיה ותהליכים

5.3. **מדדי מחיר**

5.3.1. מציע במכרז נדרש לתת הצעת מחיר בהתאם למפורט ב"טופס הצעת המחיר" (ראה נספח 1 בפרק ב׳ של המכרז).

5.3.2. עבור כל יחידת תמחור שתופיע בטופס הצעת המחיר יחושב ציון, בהתאם לנוסחאות המפורטות מטה.

5.3.3. השוואת מחירי ההצעות תתבצע על בסיס עיקרון "עלות למזמין". קרי, העלות הסופית שנדרש המזמין לשלם בגין כל הצעה. כך, לשם השוואת ההצעות וחישוב ציון ההצעה, יובא בחשבון המחיר הסופי למזמין כפי שהופיע בטופס הצעת המחיר.

5.4. **אופן חישוב הניקוד**

5.4.1. **אופן חישוב ציון האיכות:** עבור כל מציע יחושב ציון איכות בהתאם לסכימת כלל הציונים שקיבל המציע בכל תבחין איכות בהתאם למשקל של אותו תבחין.

5.4.2. **אופן חישוב ציון המחיר:** עבור כל מציע, חישוב ציון המחיר ייעשה באופן הבא:

5.4.2.1. ראשית תחושב הצעת המחיר המשוקללת על פי השלבים הבאים:

5.4.2.1.1. חישוב הצעת המחיר המשוקללת יעשה באמצעות הכפלת מחיר כל אחת מיחידות התמחור במשקל היחסי של אותה יחידה, כמוגדר בטופס הצעת המחיר וסכימת כלל היחידות.

5.4.2.1.2. לאחר חישוב הצעת המחיר המשוקללת יינתן ציון בגין הצעת המחיר בהתבסס על הנוסחה המפורטת להלן:

$$\mathbf{PS_i = 100 \times (1 - \frac{P_i - P_{min}}{P_{max}})}$$

5.4.2.1.2.1. הגדרות:

5.4.2.1.2.1.1. ציון המחיר של מציע i - PS_i

5.4.2.1.2.1.2. הצעת המחיר המשוקללת של מציע i - P_i.

5.4.2.1.2.1.3. הצעת המחיר המשוקללת הנמוכה ביותר שהתקבלה על ידי מי מהמציעים – P_{min}

5.4.2.1.2.1.4. הצעת המחיר המשוקללת הגבוהה ביותר שהתקבלה על ידי מי מהמציעים – P_{max}

5.4.3. **ציון ההצעה המשוקלל ייעשה בהתאם לנוסחה הבאה:**

5.4.3.1. $Gi = 70\% \times TQi + 30\% \times PSi$

5.4.3.2. **הגדרות:**

5.4.3.2.1. ציונה המשוקלל של ההצעה i - G_i

5.4.3.2.2. ציון האיכות של מציע i בהתאם למפורט מעלה – TQ_i

5.4.3.2.3. ציון המחיר של ההצעה i בהתאם למפורט מעלה – PS_i

6. בחירת זוכה

6.1. דירוג ההצעות

6.1.1. ההצעות ידורגו בהתאם לציון שהתקבל לאחר שקלול אמות המידה הקבועות במכרז, כאשר ההצעה בעלת הציון הגבוה ביותר תדורג ראשונה, לאחריה ההצעה עם הניקוד השני בטיבו, וכן הלאה.

6.1.2. אם לאחר שקלול ההצעות כמפורט לעיל, ההצעות בעלות הציון המשוקלל הגבוה ביותר קיבלו ציון זהה, יפעל המזמין לפי סדר הפעולות הבא עד לבחירת זוכה:

יפעל בהתאם להוראות סעיפים 2ב ו-2ד לחוק חובת המכרזים, התשנ"ב-1992, בדבר "עסק בשליטת אישה" ובדבר "עידוד משרתי מילואים בעסקים זעירים, קטנים או בינוניים" כהגדרתם שם, וזאת בתנאי שהמציע עומד בדרישות החוק.

אם עדיין אין הכרעה, ההצעה בעלת ציון האיכות הגבוה ביותר תדורג ראשונה.

6.1.2.1. אם עדיין אין הכרעה, יבצע המזמין הליך תיחור נוסף, בין אותן הצעות, במסגרתו כל אחד מהמציעים יוכל להגיש הצעת מחיר מטיבה ביחס להצעתו המקורית או לחלופין לבצע הגרלה בין אותן הצעות על מנת לקבוע את דירוגן, בהתאם לשיקול דעת המזמין.

6.2. בחירת זוכה

6.2.1. בתום דירוג ההצעות כמפורט לעיל, המזמין יכריז על המציע שהצעתו דורגה ראשונה, כזוכה במכרז, בכפוף לביצוע הפעולות המפורטת להלן ("**זוכה**"), וכן יודיע למציעים האחרים על ההכרזה כאמור.

6.3. כשירים לזכיה

6.3.1. המזמין יהיה רשאי לבחור כשירים במכרז ("**הכשיר**"), וזאת בהתאם לסדר דירוג ההצעות במכרז. אם תבוטל זכייתו של זוכה במכרז, מכל סיבה שהיא, בתקופה שעד תום שנה מיום בחירתו כזוכה, רשאי המזמין להכריז על הכשיר הבא אחריו כזוכה בכפוף לעמידה בדרישות המנויות להלן בנוגע לזוכה במכרז.

6.3.2. מציעים שיוגדרו ככשירים במכרז יידרשו להעמיד ערבות כשיר בגובה של 50,000 ₪, וזאת תוך פרק זמן שיוגדר על ידי המזמין. תוקף ערבות הכשיר יהיה 12 חודשים מיום הבחירה במציע ככשיר.

6.4. תנאים לחתימה על הסכם ההתקשרות עם הזוכה

6.4.1. כתנאי לחתימת המזמין על הסכם ההתקשרות, על הזוכה לבצע את הפעולות הבאות, בפרק זמן שיוגדר על ידי המזמין:

6.4.1.1. אם הזוכה הוא חברה, למעט חברה ממשלתית, עליו להעביר אישור מעודכן כי החברה אינה רשומה כמפרת חוק ואינה מצויה בהתראה לפני רישום כחברה מפרת חוק. ניתן להיעזר באתר הגיידסטאר.

6.4.1.2. אם הזוכה הוא עמותה, הקדש, אגודה עותומאנית או חברה לתועלת הציבור –

6.4.1.2.1. הגשת אישור ניהול תקין מאת רשם העמותות או רשם ההקדשות, לפי העניין, המעיד כי הגוף מקיים את דרישות חוק העמותות, התש"ם-1980, חוק החברות, התשנ"ט-1999 או חוק הנאמנות, התשל"ט-1979 או החוק העותומני על האגודות (1909), לפי העניין, והנחיות רשם העמותות/רשם ההקדשות, לפי העניין, לאופן ניהולו התקין לצורך קבלת האישור, למעט החריגים הבאים, בהם ניתן יהיה להסתפק ב"אישור הגשת מסמכים" מאת הרשם הרלוונטי:

6.4.1.2.1.1. התקשרות עם עמותה, חל"צ, או ההקדש, אשר טרם חלפו שנתיים מיום רישומן.

6.4.1.2.1.2. התקשרות עם אגודה עותומאנית.

6.4.1.2.2. זוכה אשר הצהיר במסגרת הצעתו כי הוא אינו חב בתשלום מע"מ במסגרת ביצוע ההתקשרות ושהוא פנה לרשות המיסים לקבלת אישור על כך, יגיש אישור מאת רשות המיסים על כך שהוא פנה אליהם לקבלת אישור כאמור.

6.4.1.3. להגיש את הסכם ההתקשרות שב**פרק ד**, על נספחיו (לדוג' נספח ערבות בנקאית לטובת ביצוע ההתקשרות ("**ערבות ביצוע**"), נספח סודיות והיעדר ניגוד עניינים וכדו') כשהוא חתום על ידי הזוכה.

6.4.2. אם הזוכה לא הצליח לבצע את הפעולות המנויות לעיל בסד הזמנים שהוגדר על ידי המזמין, יוכל המזמין, בהתאם לשיקול דעתו הבלעדי, לתת לו ארכה להשלים את ביצוע הפעולות, לפסול את הצעתו ולבטל את המכרז, או להכריז על המדורג הבא כזוכה במכרז.

6.5. **תחילת מתן השירותים**

6.5.1. לאחר שימלא הזוכה את כל התנאים הנקובים יוסיף המזמין את חתימת מורשי החתימה מטעמו על גבי הסכם ההתקשרות ("**מועד החתימה על הסכם ההתקשרות**").

6.5.2. על הזוכה להיות מוכן לתחילת העבודה, וזאת תוך 14 ימים ממועד החתימה על הסכם ההתקשרות.

7. מופעים ומועדים במכרז

7.1. מועדי המכרז

7.1.1. הליך המכרז יתבצע, בהתאם ללוח הזמנים המפורט להלן:

נושא	תאריך
כנס מציעים	01/07/2026 בשעה **10:00**
מועד אחרון להגשת שאלות הבהרה	ב 08/07/2026 בשעה **12:00**
מועד תחילת הגשת הצעות	ב 06/08/2026 בשעה **08:00**
מועד אחרון להגשת הצעות	ב 13/08/2026 בשעה **14:00**

7.1.2. הזמנים המפורטים בטבלה מחייבים את כל מי שמעוניין להתמודד במכרז. שינוי לוחות הזמנים יתבצע על ידי המזמין בלבד, ובהתאם לשיקול דעתו הבלעדי.

7.1.3. כל שינוי במועדי המכרז או עדכונים הנוגעים להם יפורסמו באתר האינטרנט של מינהל הרכש הממשלתי בכתובת: www.mr.gov.il תחת שם המכרז – מכרז 11/2026 – לאפיון, הקמה והתפעול של מרכז ניטור ותגובה סייבר במגזר התחבורה (TSOC) ("**דף המכרז**").

7.2. כנס מציעים

7.2.1. השתתפות בכנס המציעים <u>אינה</u> מהווה תנאי להשתתפות במכרז, אולם מציע אשר לא ישתתף בכנס, יהיה מנוע מלטעון כי הוא לא קיבל מידע שניתן במהלך הכנס.

7.2.2. יש להירשם מראש לכנס באמצעות שליחת שם הנציג שישתתף מטעם המציע בכנס לכתובת המייל agafcybersec@mot.gov.il . כל נציג שישתתף בכנס יוכל לייצג מציע אחד בלבד.

7.2.3. כנס המציעים יתקיים באופן מקוון. קישור לכנס יישלח למי שנרשם מראש, כמפורט לעיל. כנס המציעים המקוון יתנהל בהתאם לכללים שיקבע המזמין.

7.2.4. תשובות שיינתנו בכנס המציעים יחייבו את המזמין רק אם ניתנו בכתב והועברו לכלל המציעים בהתאם למפורט להלן.

7.3. שאלות הבהרה בנוגע למכרז

7.3.1. בכל מקרה של אי בהירות או הערות בנוגע למכרז, מועדיו או לתנאיו ניתן לפנות למזמין בשאלות הבהרה, וזאת עד למועד האחרון להגשת שאלות הבהרה הנקוב לעיל.

7.3.2. שאלות הבהרה יוגשו באמצעות מערכת יהלום. מציע אשר מעוניין לשאול שאלות הבהרה, נדרש ללחוץ על הקישור המתאים בדף המכרז ולפעול בהתאם להנחיות במערכת. שאלות שיועברו לאחר המועד הנקוב לעיל, או שיועברו שלא באמצעות מערכת יהלום, לא יחייבו מענה מאת המזמין.

7.3.3. המזמין רשאי לאפשר סבבים נוספים של שאלות הבהרה, בהודעה שתפורסם בדף המכרז, וזאת בהתאם לשיקול דעתו הבלעדי.

7.3.4. מציע שלא יפנה למזמין בשאלות הבהרה על המכרז, בהתאם לכללי המכרז, יהיה מנוע מלהעלות בעתיד כל טענה, דרישה או תביעה כנגד המכרז.

7.4. מענה המזמין לשאלות ההבהרה

7.4.1. תשובות והבהרות תינתנה בכתב בלבד, נוסחן הוא הנוסח המחייב והן יהיו חלק בלתי נפרד ממסמכי המכרז.

7.4.2. תשובות והבהרות של המזמין, יפורסמו בדף המכרז. באחריות מציע במכרז להתעדכן בתשובות המזמין וכן בעדכונים שוטפים אשר יפורסמו בנוגע למכרז זה.

7.4.3. המזמין רשאי לבצע כל שינוי במסמכי המכרז, וכן ליתן פרשנות או הבהרה להוראות מסמכי המכרז.

7.4.4. המזמין אינו מחויב לנוסח שאלה שהוגשה, ובכלל זה רשאי המזמין, בעת ניסוח מענה לשאלות ההבהרה, לקצר נוסח שאלה או לנסחה מחדש.

7.4.5. תשובות המזמין יפורסמו ללא שמות הפונים.

7.5. הגשת הצעות במכרז

7.5.1. הגשת ההצעות למכרז תבוצע באופן מקוון, באמצעות מערכת יהלום, אלא אם כן קבע המזמין, בהודעה שתפורסם בדף המכרז, דרך הגשה אחרת במכרז. במקרה כאמור על המציעים לפעול בהתאם להוראות להגשת הצעות שפרסם המזמין בדף המכרז.

7.5.2. הצעת המחיר (נספח 1 לפרק זה) תוגש כקובץ נפרד מחוברת ההצעה בהתאם להוראות המפורטות במערכת להגשת הצעות בקשר עם מכרז זה. מודגש בזה שפרטי הצעת המחיר או העתק ממנה לא יופיעו בחוברת ההצעה בשום דרך שהיא.

7.5.3. קישור למערכת יהלום לצורך הגשת הצעות במכרז יפורסם בדף המכרז. מציע המעוניין להגיש את הצעתו במכרז נדרש ללחוץ על הקישור "להגשת הצעות", אשר יעביר אותו למערכת.

7.5.4. הליך הגשת ההצעות במערכת כולל 2 שלבים: 1) הזדהות מגיש ההצעה באמצעות מערכת ההזדהות הממשלתית; 2) הגשת ההצעה בתיבת המכרזים במערכת יהלום ("**התיבה**").

7.5.5. פעולות במערכת ההזדהות -

7.5.5.1. מגיש הצעה אשר טרם נרשם למערכת ההזדהות הממשלתית יידרש להירשם למערכת, ולאחר השלמת ההרשמה לערוך אימות של ההזדהות לצורך מעבר לשלב הגשת ההצעות.

7.5.5.2. מגיש הצעה אשר רשום למערכת ההזדהות הממשלתית, יידרש לאמת את זהותו לצורך מעבר לשלב הגשת ההצעה.

7.5.5.3. בכל תקלה בהליך ההרשמה להזדהות הממשלתית, או בתהליך ההזדהות יש לפנות למוקד התמיכה של המערכת (טלפון - 1299, כתובת דואר אלקטרוני moked@mail.gov.il, טלפון נוסף 08-6863100).

7.5.5.4. לפרטים נוספים אודות הליך ההרשמה ראו בקישור זה.

7.5.5.5. לאחר השלמת ההזדהות, המערכת תעביר את מגיש ההצעה באופן אוטומטי לתיבת המכרז הרלוונטית. על המציע לוודא כי במערכת להגשת ההצעות מופיע שם ומספר המכרז המבוקש על ידו.

7.5.6. פעולות במערכת יהלום -

7.5.6.1. במסגרת הגשת ההצעה על המציע לפעול בהתאם להנחיות שיופיעו במערכת יהלום, למלא את כלל השדות שנדרש באופן ברור ובהתאם להנחיות המערכת, ולהעלות למערכת את הקבצים הנדרשים בהתאם להוראות המכרז.

7.5.6.2. מציע יוכל לעדכן את הצעתו כל עוד לא חלף המועד האחרון להגשות הצעות.

7.5.6.3. לאחר השלמת הגשת ההצעה במערכת תתקבל הודעה "הצעתך נשלחה בהצלחה" ומציע יוכל להוריד את מסמך ההצעה. מסמך ההצעה הינו מסמך חתום דיגיטלית של ההצעה ומהווה אסמכתא להצעה שהוגשה. המסמך ישלח למציע גם בדואר האלקטרוני. מסמך ההצעה האחרון שנשלח יוצג גם במערכת בדף הבית של המכרזים באזור "הצעות שנשלחו".

7.5.6.4. לא ניתן יהיה להגיש הצעות במערכת לאחר המועד האחרון להגשת הצעות.

7.5.6.5. במסגרת הגשת ההצעות במערכת, ישנן מגבלות טכניות שונות, כגון:

7.5.6.5.1. ניתן להעלות עד 10 קבצים כאשר הגודל המקסימלי של כל קובץ הוא עד 15MB. ניתן לעלות קבצים מהסוגים הבאים: jiff, pjpeg, pjp, tiff, tif, doc, docx, xls, xlsx, ppt, pptx, pdf, png, jpg, jpeg. לא ניתן

לעלות קבצים עם שמות זהים, מומלץ לתת לכל קובץ שם קצר בהתאם לתכולה שלו.

7.5.6.5.2. פרק הזמן שבו המערכת מתנתקת בהיעדר פעולה של משתמש הוא עשרים דקות.

7.5.6.6. על מנת להכיר את יתר מגבלות המערכת,באחריות מגיש ההצעה לקרוא מבעוד מועד את המדריך להגשת הצעות בתיבה הדיגיטלית.

7.5.6.7. לסיוע טכני במקרה של תקלה או שאלה ניתן לפנות למוקד התמיכה בימים א'-ה' בין השעות 8:00-17:00 באמצעות הצ'אט האנושי. יש לציין בפניה את שם המכרז, המועד האחרון להגשת ההצעות ובמידת הצורך לצרף צילומי מסך.

7.5.6.8. זמן ההמתנה מרגע משלוח הפניה ועד לחזרת נציג שירות לא יעלה על 4 שעות בטווח שעות פעילות המוקד. מוקד התמיכה אינו מתחייב לספק מענה לפניות אשר יתקבלו בזמן קצר מ-4 שעות מהמועד האחרון להגשת הצעות. **מציע אשר מגיש את הצעתו כאשר ישנן פחות מ-4 שעות להגשת הצעות במכרז לוקח על עצמו את הסיכון שבמקרה של תקלה נציג השירות לא יספיק לפתור את הבעיה הטכנית שלו או לענות על שאלה שיש לו**.

7.5.6.9. על מציע במכרז האחריות הבלעדית להגיש את ההצעה לפני המועד האחרון להגשת הצעות. על המציע להביא בחשבון כי בסמוך למועד האחרון להגשת הצעות ייתכן עומס על מערכת ההגשה או תקלות טכניות אחרות אשר ימנעו מהמציע להגיש את הצעתו. **על המציע להיערך לכך, ולהגיש את הצעתו מבעוד מועד**. למציע לא תהיה כל טענה למזמין באשר לתקלה שהתגלתה במערכת ההזדהות או במערכת הגשת ההצעות סמוך למועד האחרון להגשת הצעות, גם אם כתוצאה מכך הוא לא הצליח להגיש את הצעתו במכרז.

7.6. ביטול אוטומטי של הצעה שהוגשה – תיקונים במסמכי המכרז

7.6.1. כמפורט לעיל, שינויים במסמכי המכרז יתכנו עד למועד האחרון להגשת הצעות ואף לאחר המועד ממנו ניתן להתחיל להגיש הצעות למכרז. אם לאחר שהוגשה הצעה לתיבה, ערך המזמין שינוי במסמכי המכרז, למעט שינוי במועדי המכרז, הצעה שהיתה בתיבה תבוטל באופן אוטומטי ותעבור למצב טיוטה. מציע אשר יהיה מעוניין להגיש את הצעתו בהתאם לתנאי המכרז המעודכנים יידרש לבצע הגשה מחדש.

7.6.2. באחריותו הבלעדית של המציע להתעדכן בסטאטוס הצעתו במערכת הגשת ההצעות.

8. כללי המכרז

8.1. בדיקת ההצעות

8.1.1. המזמין יבדוק כי המציע הגיש את ההצעה בהתאם להנחיות המכרז וצירף את כל המסמכים כנדרש בחוברת ההצעה (פרק ב), וינקד את ההצעות בהתאם לאמות המידה המפורטות במכרז.

8.1.2. במקרה בו המציע, כאישיות משפטית עצמאית, אינו עומד בתנאי הסף המפורטים לעיל, או בתנאים אחרים הקבועים במכרז, ובעברו של המציע התרחש שינוי ארגוני (לדוגמא רכישת פעילות, התאגדות כחברה, רה-ארגון או איחוד של חברות בדרך אחרת), באופן בו הפעילות הרלוונטית לצורך עמידה בתנאי המכרז השתלבה אצל המציע. במקרה כאמור יוכל המציע לבקש מהמזמין בכתב ובאופן מנומק לצרף לנתוניו את נתוני הגוף בו התקיימה הפעילות לפני השינוי הארגוני. החלטה בדבר הכרה כאמור תהיה בכפוף לשיקול דעת המזמין.

8.1.3. בחינת רלוונטיות של עבר פלילי לנושא המכרז תיעשה על ידי ועדת המכרזים בהתאם לשיקולים המפורטים בהוראת תכ"ם 7.3.4 "התחשבות במידע פלילי במסגרת הליכי רכש".

8.1.4. לצורך בדיקת ההצעות וניקודן רשאי המזמין לעשות שימוש בצוות מקצועי אשר יכול ויכלול גם יועצים חיצוניים.

8.1.5. המזמין רשאי לבקש ממציע לבאר פרט מסוים מתוך הצעתו, להשלים בה פרט חסר, או להמציא מסמך נוסף או חלופי המוכיח את עמידתו בתנאי המכרז, ובפרט בתנאי הסף של המכרז, וזאת בתוך פרק זמן קצוב. אי מענה לפניה כאמור, או מענה שלא בפרק הזמן שהוגדר עלול לגרום לפסילת ההצעה, בהתאם לשיקול הדעת של המזמין.

8.1.6. אם הוחלט על מתן אפשרות למציע לבצע השלמה של הצעתו, המזמין רשאי לפסול הצעה שעדיין אינה עונה על דרישות המכרז או, בהתאם לשיקול דעתו לבקש השלמה נוספת.

8.1.7. אם ימצא בעת בחינת ההצעות כי ההצעה כוללת התנאה או הסתייגות על תנאי המכרז, התנאה או הסתייגות זו לא תזכה להכרה מצד המזמין ועשויה אף להביא לפסילת ההצעה בהתאם לשיקול דעתו הבלעדי של המזמין.

8.1.8. לצורך בדיקה ומתן ניקוד להצעות יעשה המזמין שימוש במידע המפורט בהצעה שהגיש המציע וכן הוא רשאי לעשות שימוש במקורות מידע מהימנים אחרים וביניהם הידע המקצועי העומד לרשותו של המזמין, וכן לעשות שימוש בניסיון העבר של המזמין עם המציע או של גוף ממשלתי אחר עם המציע, אם קיים ניסיון כאמור, במידע ציבורי על המציע, בחוות דעת יועצים מקצועיים, וכיוצא באלה. יודגש, לצורך ניקוד ההצעות, המזמין יהיה רשאי להתחשב בניסיון שלו עם

המציע או של גוף ממשלתי אחר, וזאת במקום או בנוסף ללקוחות אחרים שפורטו בהצעה, אם פורטו או במסגרת כל אמת מידה רלוונטית אחרת.

8.1.9. בדיקת ההצעות במכרז תתבצע באופן הבא – ראשית יבדקו ההצעות ללא הצעת המחיר, רק לאחר סיום שלב זה יפתח המזמין את מעטפות הצעת המחיר.

8.2. ניהול מו"מ עם מציעים

8.2.1. המזמין יהיה רשאי, בהתאם לשיקול דעתו הבלעדי, לנהל משא ומתן עם המציעים במכרז לצורך קבלת הצעה אשר מטיבה עם המזמין.

8.2.2. משא ומתן עם מציעים, אם יתקיים, ינוהל בהתאם לתקנה 7 לתקנות חובת המכרזים.

8.3. הצעה יחידה

8.3.1. אם הוגשה במכרז הצעה יחידה או שלאחר בדיקת ההצעות נותרה הצעה אחת בלבד, המזמין, בהתאם לשיקול דעתו הבלעדי יהיה רשאי:

8.3.1.1. להכריז על המציע שנותר כזוכה;

8.3.1.2. לבטל את המכרז, ולצאת למכרז חדש.

8.4. פסילת הצעות

8.4.1. המזמין, יהיה רשאי לפסול הצעה שהוגשה במכרז, לפי שיקול דעתו, ובמקרים המתאימים לאחר שנתן למציע זכות טיעון (בכתב או בע"פ, בהתאם לקביעתו הבלעדית של המזמין), בין היתר, אם מתקיים אחד מהתנאים הבאים:

8.4.1.1. **הצעה הפסדית**– אם ההצעה הינה בלתי כלכלית למציע במידה המטילה בספק את יכולתו לעמוד בהתחייבויותיו היה ויזכה במכרז.

8.4.1.2. **הצעה תכסיסנית או הצעה המוגשת בחוסר תום לב** – אם ההצעה כוללת מחירים או הנחות חריגות, סבסוד צולב, dumping וכל מקרה אחר שבו ההצעה נגועה בחוסר תום לב, ובכלל זה במקרה של פעולה או התנהגות של המציע, במסגרת המכרז, שלא בתום לב.

8.4.1.3. **התנהגות במכרזים ובהתקשרויות קודמות** – המציע, במסגרת מכרז או התקשרות קודמת של המזמין, או של משרד ממשלתי ויחידת סמך אחרים, נהג בחוסר תום לב, בערמה, בתכסיסנות או בחוסר ניקיון כפיים, מסר מידע מטעה או מידע מהותי בלתי מדויק או התנהל בחוסר מקצועיות קיצונית, באופן שלדעת המזמין מצדיק את פסילתו.

8.4.1.4. **מצב כלכלי של המציע** – אם עקב מצבו הכלכלי הנוכחי או הצפוי של המציע, לרבות הליכי פשיטת רגל או פירוק או תביעות מהותיות הקיימות נגדו, קיים חשש לתיפקודו באם יזכה במכרז.

8.4.1.5. **ניגוד עניינים** – אם קיים ניגוד עניינים, ישיר או עקיף, או חשש לניגוד עניינים בין ענייני המציע, ההצעה שהוא הגיש, או בעלי העניין בו, לבין השתתפות וזכיה במכרז או ביצוע השירותים על ידי המציע, באופן שלדעת המזמין, בהתאם לשיקול דעתו הבלעדי, אינו ניתן להסדרה.

8.4.1.6. **תיאום הצעות** - אם קיים חשד סביר לתיאום בין המציע להצעות אחרות במכרז, או בין המציע לבין מציע פוטנציאלי.

8.5. מינוי נציג מטעם המציע

8.5.1. לצורך המכרז ימנה המציע נציג מטעמו (כמפורט בפרק ב) אשר יהווה את הכתובת הבלעדית לכל פניה בנושא המכרז.

8.5.2. כל מענה והתייחסות שתישלח מנציג המציע למזמין, או מהמזמין לנציג המציע תחייב את המציע.

8.6. תוקף הצעות

8.6.1. תוקף ההצעה הוא 90 יום לאחר המועד האחרון להגשת הצעות. המזמין רשאי להודיע על הארכת תוקף ההצעה לתקופה נוספת של עד 90 ימים, זאת לצורך בחירת זוכה במכרז.

8.6.2. מציע אינו רשאי לחזור בו מהצעתו בתקופה בה הצעתו בתוקף.

8.7. ביטול או שינוי המכרז

8.7.1. המזמין רשאי מיוזמתו ועל פי שיקול דעתו הבלעדי, לבטל את המכרז, לשנותו ולעדכנו, לרבות עדכוני מועדים הנקובים בו ופרסום הבהרות על האמור בו.

8.7.2. הודעה על ביצוע שינויים כאמור תפורסם בדף המכרז. על מציע האחריות להתעדכן באופן עצמאי בהודעות ועדכונים אשר יפורסמו כאמור בנוגע למכרז זה.

8.7.3. ההתקשרות עם הזוכה במכרז מותנית בקיומו של תקציב זמין. אם מסיבות תקציביות לא ניתן יהיה להתקשר עם הזוכה במכרז, רשאי המזמין לבטל את המכרז.

8.7.4. המזמין לא יהיה חייב לפצות את המציעים במקרה של ביטול המכרז.

8.8. יועצים שסייעו למזמין בכתיבת המכרז

8.8.1. לצורך כתיבת המכרז המזמין עשה שימוש ביועצים הבאים:

8.8.1.1. KPMG סומך חייקין

8.8.2. יועצים אלו מנועים מלקחת חלק במכרז, ולא יכולים לתת ייעוץ למציעים במכרז.

8.8.3. מציעים אשר יסתייעו ביועצים אלו לצורך הגשת הצעות במכרז, בין בתשלום ובין ללא תשלום, הצעתם תיפסל, בכפוף לשימוע.

8.9. **הוצאות**

8.9.1. מציעים הבוחרים להגיש הצעה במכרז יישאו בכל עלות כספית הנדרשת לצורך השתתפותם במכרז, ולא יהיו זכאים להחזר כלשהו מהמזמין בגין עלויות אלו.

8.9.2. המציעים לא יהיו זכאים להחזר הוצאות או לפיצוי כלשהו בקשר עם המכרז, לרבות במקרה של הפסקתו, עיכובו, שינוי תנאיו או ביטולו.

8.10. **סמכות השיפוט**

8.10.1. סמכות השיפוט בכל הקשור לנושאים ועניינים הנוגעים למכרז, או בכל תביעה הנובעת מהמכרז ומניהולו, תהיה אך ורק בבתי המשפט במקום בו יושבת ועדת המכרזים של המזמין.

8.11. **סודיות ההצעה וזכות העיון**

8.11.1. בכפוף לחובות המזמין על פי דין, המזמין מתחייב שלא לגלות תוכן ההצעה לצד שלישי שאינו מעובדי המזמין או יועצים המועסקים על ידו ונותנים לו שירות לצורך המכרז, אשר גם עליהם תחול חובת הסודיות ואי השימוש בהצעות שהוגשו במכרז אלא לצורכי המכרז בלבד.

8.11.2. יחד עם זאת, בהתאם לתקנה 21(ה) לתקנות חוק חובת המכרזים, מציעים במכרז רשאים לבקש לעיין בהצעה זוכה, וכן בפרוטוקולים של ועדת המכרזים ובמסמכים נוספים הקשורים במכרז (או חלקם), מלבד החריגים המנוים בתקנה, ובכלל זה במסמכים שהם בגדר סוד מסחרי או מקצועי, או שעלולים לפגוע בביטחון המדינה, יחסי החוץ שלה, כלכלתה וביטחון הציבור.

8.11.3. בהתאם לאמור בתקנות המידע הפלילי ותקנת השבים (מסירת מידע מהמרשם הפלילי לשם התקשרות בחוזה לביצוע עסקה במסגרת מכרז), התשפ"ה-2025 ("**תקנות מידע פלילי במכרזים**"), אשר הותקנו מכוח חוק המידע הפלילי ותקנת השבים, תשע"ט-2019, מובהר כי ועדת המכרזים לא תחשוף מידע פלילי של מציע במסגרת בקשה לעיון בהצעות במכרז, לרבות את עצם קיומו.

8.11.4. אם ברצון מציע למנוע עיון בסעיפים של הצעתו בשל טענה לסוד מסחרי, סוד מקצועי, או כל טעם אחר המוזכר בתקנות חובת המכרזים עליו לציין זאת באופן מפורש בחוברת ההצעה (פרק ב), במקום המיועד לכך. מובהר כי לא יהא בעצם הבקשה כדי למנוע עיון בסעיפים הרלוונטיים, והחלטה בנושא תתקבל על ידי ועדת המכרזים של המזמין. מובהר כי מחיר ההצעה אינו בגדר סוד מסחרי או מקצועי.

8.11.5. מציע שטען שחלק מסוים מהצעתו הוא סוד מסחרי או מקצועי, יהיה מנוע מלדרוש לעיין בחלק זה של ההצעה הזוכה במכרז.

8.11.6. בכפוף לאמור לעיל, בהשתתפותו במכרז מסכים המציע, כי במקרה של זכיה במכרז הצעתו תועמד לעיונם של יתר המציעים במכרז בהתאם להוראות הדין ולא יהיו לו כל טענות בקשר לגילוי פרטי הצעתו בהתאם להוראות סעיף זה.

8.11.7. במקרה בו ועדת המכרזים של המזמין תדחה את טענת המציע הזוכה בדבר היות חלקים מהצעתו סוד מסחרי או מקצועי, המזמין יודיע לו על כך טרם מימוש זכות העיון בפועל.

8.12. **מיצוי הליכים מול הוועדה**

8.12.1. אם לאחר מימוש זכות העיון, מציע במכרז סבור שנפלה טעות בהחלטה של ועדת המכרזים, עליו לפנות לוועדה בכתב ולפרט את טענותיו באופן מנומק וזאת לא יאוחר מ-10 ימי עסקים ממועד מימוש זכות העיון.

8.12.2. במהלך בירור טענות מציע במכרז, אם ישנן, המזמין לא יעכב את מימוש ההתקשרות עם הזוכה, למעט מקרים חריגים, בהתאם לשיקול דעתו הבלעדי.

8.12.3. אם לאחר בירור טענות המציע, ועדת המכרזים, תסבור כי נפלה טעות בהחלטה שקיבלה, לא יהיה במימוש ההתקשרות עם הזוכה כדי למנוע ממנה לקבל כל החלטה נדרשת לצורך תיקון הטעות, ובכלל זה, במקרים חריגים, ביטול הזכייה.

פרק ב' – חוברת ההצעה

9. הגשת הצעה במכרז

9.1. כללים למילוי חוברת ההצעה

9.1.1. פרק זה מהווה את מענה המציע למכרז, אין צורך במתן מענה לכל חלק אחר במכרז, או לצרף מסמך שאינו נדרש בפרק זה.

9.1.2. יש לעקוב באופן מדוקדק אחר ההנחיות המופיעות בפרק זה על מנת שההצעה תוכל להיבחן ולהיות מוערכת כראוי. אין להוסיף להתנות או לשנות אף תנאי מתנאי המכרז, או את ההנחיות המופיעות להלן.

9.1.3. בכל מקרה של שאלות או אי-בהירות במסמכי המכרז על המציע לפנות למזמין בשאלה לצורך הבהרה, כמפורט ב**פרק א'** למסמכי המכרז.

9.1.4. ניתן לצרף כל מסמך או קובץ הרלוונטי לצורך פירוט והמחשה למפורט בהצעה. יודגש כי בדיקת ההצעה, תתבסס על הפירוט שיינתן בחוברת ההצעה.

9.1.5. חוסר פירוט בהצעה או פירוט מיותר שאינו עונה לדרישת המכרז, עלולים להביא לניקוד נמוך של ההצעה או פסילתה בהתאם לשיקול דעתו הבלעדי של המזמין.

10. פרטי המציע

שם המציע	
סוג מציע (תאגיד/שותפות/עמותה/עוסק מורשה וכדו')	
תאריך הרישום במרשם (אם רלוונטי)	
מספר מזהה (לדוג' ח"פ)	

10.1. פרטי איש הקשר מטעם המציע

שם:
כתובת:

טלפון:
דוא"ל:

11. הוכחת עמידה בתנאי הסף של המכרז

11.1. בהתאם לאמור בפרק זה המציע יפרט את עמידתו בתנאי הסף שפורטו במכרז.

11.2. **הוכחת עמידה בתנאי הסף המנהליים:**

11.2.1. המציע מצהיר ומתחייב כי הוא עומד בתנאי הסף המנהליים המפורטים ב**פרק א'** למכרז ובהתאם לפירוט המובא להלן:

11.2.1.1. **מציע רשום כדין (יש לסמן ב- X את האפשרות הנכונה) –**

☐ המציע רשום בישראל כדין.

☐ לא חלה על המציע חובת רישום בישראל, על פי דין. נימוק: _____

11.2.1.2. **עמידה בחוק עסקאות גופים ציבוריים –**

11.2.1.2.1. **ניהול פנקסים** – המציע –

11.2.1.2.1.1. מנהל את פנקסי החשבונות והרשומות שעליו לנהל על פי פקודת מס הכנסה [נוסח חדש], וחוק מס ערך מוסף, התשל"ו-1975 ("**חוק מס ערך מוסף**"), או שהוא פטור מלנהלם.

11.2.1.2.1.2. מדווח לפקיד השומה על הכנסותיו ומדווח למנהל על עסקאות שמוטל עליהן מס לפי חוק מס ערך מוסף.

11.2.1.2.2. לצורך הוכחת עמידה בתנאי סף זה על המציע לצרף אישור פקיד מורשה ולסמנו **כנספח 2.**

11.2.1.2.3. **היעדר הרשעות** –

11.2.1.2.3.1. המציע ו"בעל זיקה" אליו לא הורשעו ביותר משתי עבירות לפי חוק עובדים זרים התשנ"א - 1991 (להלן: "**חוק עובדים זרים**") וחוק שכר מינימום, התשמ"ז – 1987 (להלן: "**חוק שכר מינימום**") עד למועד הגשת

ההצעה מטעם המציע במכרז, או שהורשעו כאמור אך כבר חלפה שנה אחת לפחות ממועד ההרשעה האחרונה ועד למועד הגשת ההצעה.

11.2.1.2.4. לצורך הוכחת עמידה בתנאי סף זה על המציע לצרף את התצהיר המפורט **בנספח 3.**

11.2.1.2.5. **ייצוג הולם לאנשים עם מוגבלות** (יש לסמן ב- X את אחת מהאפשרויות) –

☐ הוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, התשנ"ח-1998 **("חוק שוויון זכויות לאנשים עם מוגבלויות")** אינן חלות על המציע.

☐ הוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות חלות על המציע והוא מקיים אותן.

11.2.1.2.5.1. במקרה שהוראות סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות חלות על המציע, יש לפרט את אופן עמידתו בדרישות החוק (<u>יש לסמן ב- X את אחת מהאפשרויות</u>):

☐ המציע מעסיק פחות מ-100 עובדים.

☐ המציע מעסיק 100 עובדים או יותר.

11.2.1.2.5.2. במקרה שהמציע מעסיק 100 עובדים או יותר (<u>יש לסמן ב- X את אחת מהאפשרויות</u>):

☐ המציע מתחייב כי אם יזכה במכרז יפנה למנהל הכללי של משרד העבודה והרווחה והשירותים החברתיים לשם בחינת יישום חובותיו לפי סעיף 9לחוק שוויון זכויות לאנשים עם מוגבלות, ובמקרה הצורך– לשם קבלת הנחיות בקשר ליישומן.

☐ המציע פנה בעבר למנהל הכללי של משרד העבודה והרווחה והשירותים החברתיים לשם בחינת יישום חובותיו לפי סעיף 9 לחוק שוויון זכויות לאנשים עם מוגבלות, ואם קיבל הנחיות ליישום חובותיו פעל ליישומן.

11.2.1.3. **המציע עומד בדרישות הרישוי והתקנים הנדרשים על פי דין לצורך ההתקשרות, אם ישנם** –

11.2.1.3.1. המזמין יהיה רשאי לבקש אישור על עמידה בתקנים או בתקנים זרים מקבילים, אם עמידה בתקן זר מקביל אפשרית בהתאם להוראות הדין.

11.2.1.4. **מידע פלילי רלוונטי** –

11.2.1.4.1. לצורך הוכחת עמידה בתנאי סף זה יש לצרף להצעה תצהיר, בהתאם לנוסח המצורף למכרז כ**נספח 4.**

11.3. **הוכחת העמידה בתנאי הסף המקצועיים:**

11.3.1. עם הגשת הצעה זו, המציע מצהיר ומתחייב כי הוא עומד בתנאי הסף המקצועיים המפורטים בפרק א' למכרז.

11.3.2. המציע יפרט את אופן עמידתו בתנאי סף המקצועיים, בהתאם למפורט להלן:

11.3.2.1. **שנות נסיון** –

11.3.2.1.1. למציע ניסיון מוכח של 4 שנים בין השנים 2021-2025:

11.3.2.1.1.1. למציע ניסיון מוכח של ארבע (4) שנים לפחות בהקמת ותפעול מערכות מחשוב ומערכות אבטחת מידע וסייבר הכוללות מספר מעגלי אבטחת מידע לוגיים וטכנולוגיים, מערכות ניטור אבטחה בתצורת On-Prem וענן, הקמת פורטל ארגוני מגזרי מאובטח או פורטל ממשלתי או צבאי.

11.3.2.1.1.2. ניסיון מוכח בהקמה של מרכז ניטור רב ארגוני מאובטח לרבות ממשלתי או צבאי.

11.3.2.1.1.3. למציע יש ניסיון מוכח של ארבע (4) שנים לפחות בתכנון והקמת פרויקטים מורכבים וחדשניים המשלבים גם מאמצים של מחקר ופיתוח בתחום הסייבר.

11.3.2.1.1.4. המציע העסיק במהלך השנים 2022-2025 צוות עובדים מקצועי בתחום הנדרש במכרז הכולל עשרה (10) עובדים מקצועיים לפחות, במקצועות המפורטים מטה בצוות ההקמה ובצוות ה-TSOC ולכל הפחות עובד אחד בעל ידע ונסיון רלוונטי מכל תפקיד המוצג.

שנת התחלה	שנת סיום	פירוט אודות הניסיון

הנחיות למילוי הטבלה:
1. יש למלא את הטבלה בהתאם לפירוט הנדרש בה, אין להוסיף מידע שאינו רלוונטי.

2. יש למלא את הטבלה בהתאם לכמות התאים המופיעים בה. ככל שימולאו יותר תאים מהנדרש יבדקו רק התאים הראשונים שימולאו.
3. ניתן להוסיף לאמור בטבלה כל מסמך או מידע רלוונטי, אשר יכול להעיד על המפורט בטבלה.

11.3.2.2. **נסיון מקצועי, היקף פעילות** –

11.3.2.2.1. המציע הינו בעל מחזור פעילות שנתי בתחום הקמת והפעלת מרכזי ניטור רב ארגוניים ו/או בכלים המוצעים בהצעתו בהיקף שנתי מינימאלי של 6 מיליון ₪ בכל אחת מהשנים 2022-2025. לצורך הוכחת סעיף זה על המציע לצרף להצעתו דו"חות כספיים מבוקרים או אישור רואה חשבון מבקר המציין את היקפי המחזור של המציע בכל אחת מהשנים האמורות, בהיקף כספי של 6,000,000 ₪ לפחות.

שנת התחלה	שנת סיום	היקף כספי	פירוט נוסף

הנחיות למילוי הטבלה:

1. יש למלא את הטבלה בהתאם לפירוט הנדרש בה, אין להוסיף מידע שאינו רלוונטי.
2. יש למלא את הטבלה בהתאם לכמות התאים המופיעים בה. ככל שימולאו יותר תאים מהנדרש יבדקו רק התאים הראשונים שימולאו.
3. ניתן להוסיף לאמור בטבלה כל מסמך או מידע רלוונטי, אשר יכול להעיד על המפורט בטבלה.

11.3.2.3. **צוות הקמה** –

11.3.2.3.1. **<u>צוות הקמה</u>** - הצוות מיומן ומנוסה שיהיה אחראי על השלבים א'- וב' כמפורטים לעיל באבני הדרך לביצוע המכרז הצוות יפעל בשיתוף עם נציג המשרד ובהכוונתו למימוש השלבים ולחפיפה מסודרת והעברת הידע לצוות ההפעלה המבצעית.

11.3.2.3.2. 1. על המציע להציג במסגרת הצעתו את נותני השירותים מטעמו אשר יעמדו בתנאי הסף המקצועיים כמפורט להלן:

11.3.2.3.3. **<u>(א) מנהל הפרויקט</u>**

11.3.2.3.3.1. מנהל הפרויקט הינו בעל תואר ראשון לפחות במדעי המחשב או מערכות מידע או הנדסה ממוסד אקדמאי

מוכר על ידי המל"ג. לצורך הוכחת סעיף זה על המציע לצרף את תעודות ההשכלה של מנהל הפרויקט.

11.3.2.3.3.2. מנהל הפרויקט הועסק על ידי המציע במהלך תקופה של שלוש (3) השנים האחרונות לפחות שקדמו למועד האחרון להגשת הצעות במכרז זה.

11.3.2.3.3.3. מנהל הפרויקט הינו בעל ניסיון מוכח בניהול של לפחות שלושה (3) פרויקטים בתחום הנדרש במכרז זה במהלך 4 השנים שקדמו למועד האחרון להגשת הצעות בהיקף כספי מינימאלי של מיליון ₪ לכל פרויקט, ומספר משתמשים מינימאלי של 20 משתמשים לכל פרויקט. מנהל הפרויקט ישמש כאיש הקשר של המציע עם המשרד ויהיה אחראי על הנושאים המקצועיים ועל הנושאים המינהליים אל מול המשרד.

11.3.2.3.4. **<u>(ב) ארכיטקט מערכות</u>**

11.3.2.3.4.1. ביצע תפקיד ארכיטקט מערכות תשתית ומערכות אבטחת מידע וסייבר במשך 5 שנים לפחות.

11.3.2.3.4.2. בעל ידע מעמיק ומוכח בתשתיות טכנולוגיות, אבטחת מידע והגנת סייבר.

11.3.2.3.4.3. בעל הסמכה בתחום תשתיות טכנולוגיות ואבטחת מידע והגנת סייבר.

11.3.2.3.5. **<u>(ג) מנתח מערכות</u>**

11.3.2.3.5.1. כ"א מנוסה בניתוח מערכות המועסק על ידי המציע במהלך תקופה של שלוש (3) השנים האחרונות לפחות שקדמו למועד האחרון להגשת הצעות במכרז זה.

11.3.2.3.5.2. כ"א מנתח המערכות הינו בעל ניסיון מוכח בהכנת אפיון מפורט מהסוג הנדרש במכרז זה שבוצע בשלושה (3) פרויקטים לפחות בהיקף מינימאלי של מיליון ₪ לכל פרויקט, וזאת במהלך שלוש (3) השנים שקדמו להגשת ההצעה.

11.3.2.3.6. **<u>(ד) אחראי תפעול והטמעה</u>**

11.3.2.3.6.1. מומחה בהקמה, הטמעה ותפעול מערכות ניטור SIEM בעל ניסיון של 5 שנים במערכות SIEM מובילות בקטגוריה.

11.3.2.3.6.2. לפחות 5 שנות ניסיון בהטמעת מערכות אבטחת מידע / IT בארגונים גדולים.

11.3.2.3.6.3. ניסיון בעבודה עם מערכות SOC קריטיות, כולל:

11.3.2.3.6.4. SIEM (Security Information and Event Management) SPLUNK, QRadar, Sentinel, ArcSight וכו'.

11.3.2.3.6.5. SOAR (Security Orchestration, Automation, and Response) Phantom, XSOAR, Swimlane וכו'.

11.3.2.3.6.6. מערכות ניהול קריאות Ticketing Systems ServiceNow, Jira, BMC Remedy וכו'.

11.3.2.3.6.7. ata Lake / Big Data Platforms Elastic Stack, Hadoop, Apache Spark, AWS S3. -

11.3.2.3.6.8. MFT (Managed File Transfer) פתרונות להעברת קבצים מאובטחת.

11.3.2.3.6.9. Workflow & Automation תהליכי אוטומציה וניהול משימות ב-SOC.

11.3.2.3.6.10. ניסיון בהתקנה, קונפיגורציה ואינטגרציה של מערכות אלו בארגונים גדולים.

11.3.2.3.6.11. ניסיון בעבודה עם API אינטגרציות, Webhooks ו-Scripting (Python, PowerShell, Bash).

11.3.2.3.6.12. ניסיון מוכח בניהול והגדרת חוקי אבטחה ב-Firewalls, IDS/IPS, WAF, DLP, EDR/XDR.

11.3.2.3.6.13. עבודה והטמעה של כלי להגנת ענן של ספק ענן מוביל (AWS,GCP,)

11.3.2.3.7. על המציע להוכיח את ניסיונם של נותני השירותים המוצעים מטעמו באמצעות מסמכים שיפרטו את הניסיון הרלוונטי לפי שנים. ביחס לכל אחד מנותני השירותים מטעמו, יצרף המציע גם את המסמכים הבאים:

11.3.2.3.7.1. קורות חיים של כ"א מנותני השירותים

11.3.2.3.7.2. תעודות המעידות על השכלה של כ"א מנותני השירותים

11.3.2.3.7.3. אסמכתאות מתאימות המעידות על ניסיון רלוונטי וותק של כ"א מנותני השירותים

11.3.2.3.7.4. רשימה מסודרת בטבלה של פרויקטים/עבודות קודמות וניסיון רלוונטי של כ"א מנותני השירותים בצירוף תיאור העבודה, מועד ביצועה, רשימת

ממליצים ואנשי קשר של גורמים ולקוחות עבורם בוצעו עבודות בצירוף פירוט דרכי ההתקשרות עמם, כמפורט להלן.

11.3.2.3.8. יובהר כי המשרד רשאי לפנות לאנשי קשר/לקוחות מהרשימה הנ"ל או ללקוחות אחרים על בסיס מידע קיים או העולה מן ההצעה או מבדיקתה על מנת להתרשם ממידת שביעות הרצון של לקוחות אלו מהשירותים שסופקו להם ע"י נותן השירותים הרלבנטי.

11.3.2.3.9. במידת האפשר, ולצורך הוכחת עמידת נותני השירותים בתנאי הסף ובדרישות הנוספות, יש לצרף דוגמאות לעבודות רלוונטיות שבוצעו על ידי מי מנותני השירותים.

11.3.2.3.10. ההחלטה האם המציע עומד בדרישת הניסיון וההשכלה, ובכלל זה ההחלטה האם הניסיון שעליו הצביע המציע הוא ניסיון בהתאם לדרישות או האם ההשכלה הינה רלוונטית לשירותים נשוא מכרז זה, נתונה לשיקול דעתה של ועדת המכרזים.

נושא/תיאור העבודה שבוצעה	תקופת/שנת ביצוע העבודה	שם הלקוח	היקף העבודה	שם איש קשר	טלפון + טלפון נייד

הנחיות למילוי הטבלה:

1. יש למלא את הטבלה בהתאם לפירוט הנדרש בה, אין להוסיף מידע שאינו רלוונטי.
2. יש למלא את הטבלה בהתאם לכמות התאים המופיעים בה. ככל שימולאו יותר תאים מהנדרש יבדקו רק התאים הראשונים שימולאו.
3. ניתן להוסיף לאמור בטבלה כל מסמך או מידע רלוונטי, אשר יכול להעיד על המפורט בטבלה.

11.3.2.4. **המוצרים המוצעים מקיימים את הדרישות הבאות (יש לסמן X במקומות המיועדים לכך):**

11.3.2.4.1. סביבת מרכז הניטור תוקם באזור ישראל במסגרת ענן הנימבוס ב- AWS או ב- GCP. לטובת העניין המציע יוגדר כספק צד ג' למכרז נימבוס ויהיה זכאי להתקשרות ישירה בתנאים נימבוס אל מול ספקי שירות הענן AWS או GCP.

11.3.2.4.2. **התבססות על מוצרים מובילים** - כלל המערכות ומוצרי ה SaaS המסופקות במענה למרכז ניטור סייבר תחבורה- כולם יהיו מהקטגוריות המובילות (ללא מוצרים נישתיים - niche players) על בסיס מדד Gartner (באחד מ-3 הדו"חות האחרונים) ויספקו את שרותיהם באזור המשילות הישראלי בהתאם להגדרות בפרויקט נימבוס.

11.3.2.4.3. יש לתת פירוט בדבר אופן העמידה בתנאי הסף (ניתן להוסיף כל מסמך רלוונטי):

_____

_____

_____

_____

11.3.2.4.4. עקרון **תכנון ענן - FinOps** המענה המוצע מתבקש להיות בתצורת מבוססת ענן - נדרש לבצע תכנון מקיף של המענה תוך התחשבות בכלכלת ענן יעילה בהתאם לעקרונות FinOps תוך ביצוע בקרה, אכיפה, משילות והתייעלות קבועה ומתמשכת ליצירת אפקטיביות אופטימלית של ההצעה בהיבט הכלכלי תוך הערכת צפי עלויות עבור כל שלבי הפרויקט. הפתרון הטכנולוגי ייקח חשבון את עקרונות" FINOPS כלכלת ענן חכמה" ותבוסס על עקרון ה OPEX-תוך יצירת ניהול משאבים הדוק עבור כל הפרויקט ותתי המרכיבים במטרה ליעילות כלכלית מקסימלית ושקיפות מלאה וקלה למקבלי ההחלטות - יוצג תחשיב עלויות מוערך על בסיס ההצעה לתקופת ההקמה, לתקופת ההפעלה ולתקופת האופציה.

11.3.2.4.5. יש לתת פירוט בדבר אופן העמידה בתנאי הסף (ניתן להוסיף כל מסמך רלוונטי):

_____

_____

_____

_____

12. איכות ההצעה

בחלק זה של ההצעה יפרט המציע את האפיון הראשוני שיבוצע עם כלל הפרטים הנדרשים בהתאם לפרק המקצועי (**פרק ג' - חלק 1 – חלק מקצועי**) לצורך הערכת איכות ההצעה על בסיס אפיון ראשוני, בהתאם למדדי האיכות שפורטו לעיל בפרק א' למסמכי המכרז. (דגש: שלב א' - "אפיון

מפורט מרכז ה "TSOC יתבסס באופן מלא על האפיון הראשוני בלבד שיוצע על ידי הספק ולכן קיימת חשיבות גבוהה לפירוט מקסימלי בשלב האפיון הראשוני שיוגש על ידי הספק בחוברת ההצעה(

12.1.1. **היישום המוצע -**

12.1.2. איכות המענה על בסיס האפיון הראשוני המפורט והמלא שיגיש המציע כחלק מהמענה על בסיס הדרישות המקצועיות (פרק ג' - חלק **1**) בדגש על:

12.1.2.1. (1) 30% - מערכת "על" -איכות פתרון הניטור (SIEM, קולקטור וכד') עפ"י הקטגוריות המובילות של גרטנר (ללא מוצרים נישתיים. אופן איסוף המידע, טיובו, דיוקו ואופן ביצוע הקורלציות לאירועים והצגתם כחלק מתמונת המצב המגזרית. Finops תכנון. **בחלק זה נדרש להדגיש ולפרט ככל הניתן גם את הפתרון למימוש בצד הג"מ שעתיד הספק לממש (טכנולוגיות, אופן איסוף המידע, אופן מיצויו והעברת המידע לסביבת מערכת העל לשם המשך עיבוד).**

12.1.2.2. (2) 10% - פתרון שו"ב מרכזי - על כלל מרכיביו - אפקטיביות ותכלול כלל המרכיבים המאפשר ניהול הטיפול באירועי סייבר, תיעוד האירועים, יכולת אחזור אירועי עבר קשורים (קורלציות) , הפקת דוחות, יצוא דוחות, תיעוד פעולות, ניהול משמרות, כלי ניהול ומודל תומך החלטה. מאגר הסייבר המרכזי ומערכת מחקר, ניתוח והעשרת מידע - תשתית מידע אחודה, מבוססת טכנולוגיית BIG DATA DATA LAKE המאפשרת לאגור את כלל המידע לטווח קצר ולטווח ארוך. תשתית המאפשרת לבצע מחקר וניתוח של אירועי סייבר מעל תשתית מאגר הסייבר המרכזי ומשתמשת ככלי ניהול, ניתוח והעשרת המידע מערכות תפעול תומכות המערכות SOAR ו- Manage File Transfer ומערכות תומכות נוספות לתפקוד המרכז TSOC.

12.1.2.3. (3) 10% - תשתיות אבטחה למרכז - מתן מענה מקיף ברמת מערכות אבטחה למרכז הסייבר אשר יספקו הגנה ואבטחה היקפית כמענה לאבטחת מרכז ה TSOC

12.1.3. **טכנולוגיה -**

12.1.3.1. איכות המענה בהתאם לאפיון הראשוני שיוגש על ידי המציע כחלק מהמענה על בסיס הדרישות הטכנולוגיות בהיבט: (1) 10% - ארכיטקטורה - ארכיטקטורה מבוססת ענן משלב פתרונות SaaS IaaS גמישה לשינויים, מבוזרת, וירטואלית ,עדכנית ושרידה הכוללת כלי ניהול, ניטור ובקרה מרכזיים, מאפשרת תחזוקה, שדרוגים ועדכונים ללא פגיעה בשרות ובזמני תגובה מהירים, ניהול גרסת מערכת, ניהול גרסאות ועדכונים, שרידות וזמינות מירבית.

12.1.3.1.1. (2) 5% - חומרה - ציוד היקפי, תחנות קצה, STORAGE, מערכת גיבוי, התקני תקשורת ואבטחת מידע, הבטחת ביצועים ושרידות וגיבוי של מקסימלית. מפרטים טכניים של ציודים וכתב הכמויות.

12.1.3.1.2. (3) 5% - תשתיות תוכנה ורישוי - מערכות הפעלה, תוכנת קצה, אפליקציות, סביבת בדיקות, סביבת פיתוח מאובטחת, ניהול גרסאות ותצורה. תחזוקה, שדרוגים ועדכונים על בסיס שנתי, תוכנות גיבוי, ממשקים מאובטחים לכניסה מרחוק רישוי תוכנות ותוכנות צד שלישי וכו'.

12.1.4. **יכולת מימוש -**

12.1.4.1. (1) 10% ניסיון המציע בפרויקטים דומים

12.1.4.2. (2) 10% התרשמות כללית והמלצות

12.1.4.3. (3) 4% מנהל הפרויקט וצוות הפרויקט, לפי:

12.1.4.3.1. • הכשרה אקדמאית

12.1.4.3.2. • הסמכה בתחום ניהול פרויקטים PMP, MPM & CIPM

12.1.4.3.3. •שנות ניסיון מוכח בדגש על פרויקטים גדולים בעולם טכנולוגיות אבטחת המידע והסייבר ובעולם התוכן הייעודי ל SOC עבור מגזר התחבורה

12.1.4.3.4. • משך עבודה בהתאם לתנאי הסף המקצועיים .

12.1.4.4. (4) 2% תכנית עבודה ולוח זמנים

12.1.4.5. (5) 4% מתודולוגיה ותפיסת הפעלה למרכז TSOC הכוללת אנשים, טכנולוגיה ותהליכים.

התחייבויות נוספות של המציע

12.2. **על הספק להבטיח נקיטת כל הפעילויות על מנת להבטיח את רציפות תפקוד המרכז והבטחת זמינות בעלי התפקידים במצבי החירום השונים בהתאם לדרישות 'פרק ג**

12.3. **כשירות להתמודדות במכרז**

12.3.1. המציע קרא בעיון רב את מסמכי המכרז על כל פרקיו, נספחיו, תנאיו וחלקיו, לרבות כל ההבהרות שפורסמו על ידי המזמין ולרבות תנאי ההתקשרות עם הספק הזוכה, הוא הבין את כל האמור בהם, ומסכים להם.

12.3.2. המציע אינו מצוי בהליכי פשיטת רגל או פירוק ולא מתנהלות נגד המציע תביעות מהותיות, שעלולות לפגוע בתפקודו אם יזכה במכרז.

12.3.3. אין מניעה לפי כל דין להשתתפות המציע במכרז.

12.3.4. אין בהגשת הצעה במכרז או בביצוע ההתקשרות נושא המכרז, על ידי המציע, כדי ליצור ניגוד עניינים, בין במישרין ובין בעקיפין, בין המציע למזמין.

12.3.5. המציע מתחייב לעדכן בכתב את המזמין, ללא דיחוי, בכל שינוי מהותי אשר חל במידע שמסר במסגרת הצעתו המכרז.

12.3.6. אם המציע אינו חב במע"מ במסגרת ההתקשרות מכוח המכרז, הוא מצהיר על כך שפנה אל רשות המסים לצורך קבלת אישור לכך, טרם הגשת הצעה במכרז.

12.4. **אי תיאום הצעות מכרז**

12.4.1. הפרטים המופיעים בהצעה זו הוחלטו על ידי המציע באופן עצמאי, ללא התייעצות, הסדר או קשר עם מציע אחר.

12.4.2. פרטי ההצעה לא הוצגו או יוצגו בפני כל אדם או תאגיד אשר מציע הצעות במכרז זה.

12.4.3. המציע לא היה מעורב בניסיון להניא מתחרה אחר מלהגיש הצעות במכרז זה, ולא היה מעורב בדרך כלשהי בהצעה שהוגשה על ידי מציע אחר.

12.4.4. המציע לא היה, ולא מתכוון להיות מעורב בניסיון לגרום למתחרה אחר להגיש הצעה גבוהה או נמוכה יותר מהצעתו זו.

12.4.5. המציע לא היה מעורב בניסיון לגרום למתחרה להגיש הצעה בלתי תחרותית מכל סוג שהוא.

12.4.6. הצעה זו מוגשת בתום לב.

12.5. עצמאות המציע

12.5.1. המציע אינו מחזיק או מוחזק על ידי מציע אחר במכרז (החזקה לעניין זה – החזקה במישרין או בעקיפין ב-25% או יותר מאמצעי שליטה, כהגדרתו בחוק ניירות ערך, התשכ"ח-1968).

12.5.2. גורם אחד אינו מחזיק ב-25% או יותר מאמצעי שליטה בו ובמציע נוסף במכרז.

12.5.3. המציע אינו קבלן משנה של מציע אחר במכרז, בקשר עם ביצוע השירותים במכרז זה.

13. בקשות

13.1. הגשת בקשות במסגרת ההצעה

13.1.1. במסגרת הצעתו רשאי המציע להגיש בקשות הנכללות בתנאי המכרז כמפורט בסעיף זה להלן וזאת כחלק בלתי נפרד מהצעתו.

13.1.2. הבקשות יכללו במסמכי ההצעה וינוסחו בצורה ברורה תוך הפנייה לסעיף אליו מתייחסת הבקשה.

13.1.3. מציע שלא יפנה למזמין בבקשה האפשרית בהתאם לכללי מכרז זה כחלק מהגשת הצעתו, יהיה מנוע מלהעלות בעתיד כל טענה, דרישה או תביעה בנושא ויראו בו כמי שויתר על בקשתו או על הזכות הנובעת ממנה, בהתאם להקשר, אף אם הוא עומד בתנאים המהותיים המקימים את הזכאות - והכל לפני העניין והקשר הדברים.

13.2. עסק בשליטת אישה

13.2.1. מציע שהוא "עסק בשליטת אישה" בהתאם להוראות סעיף 2ב לחוק חובת המכרזים ומעונין שתינתן לו העדפה יצהיר על כך כלהלן (יש לסמן X במקום המתאים): .

☐ **המציע מצהיר כי** הוא עסק אשר אישה מחזיקה בשליטה בו, ואשר יש לה, לבד או יחד עם נשים אחרות, היכולת לכוון את פעילותו וכי לא התקיים אף אחד מאלה: (1) אם מכהן ב**מציע** נושא משרה שאינו אישה – הוא אינו קרוב של המחזיקה בשליטה; (2) אם שליש מהדירקטורים אינם נשים – אין הם קרובים של המחזיקה בשליטה;

13.2.1.1. לתמיכה בהצהרה זו, **וכתנאי לקבלת העדפה** על המציע לצרף אישור רו"ח ותצהיר כהגדרתם בחוק חובת המכרזים, המעידים על כך שהעסק הוא בשליטת אישה.

13.3. עידוד משרתי מילואים

13.3.1. מציע שמחזיק בשליטה בו הוא חייל מילואים כהגדרתו בחוק שירות המילואים, התשס"ח-2008, ששירת שירות מילואים 20 ימים לפחות במהלך 12 החודשים לפני המועד האחרון להגשת הצעות במכרז, ומעונין שתינתן לו העדפה בשל כך יצהיר כלהלן (יש לסמן X במקום המתאים):

☐ **המציע מצהיר כי** הוא חייל מילואים כהגדרתו בחוק שירות המילואים, התשס"ח-2008, ששירת שירות מילואים 20 ימים לפחות במהלך 12 החודשים לפני המועד האחרון להגשת הצעות במכרז.

הוא מחזיק בשליטה בעסק מגיש ההצעה. לעניין זה "מחזיק בשליטה" – משרת מילואים פעיל שהוא נושא משרה בעסק אשר מחזיק, לבד או יחד עם משרתי מילואים פעילים אחרים, במישרין או בעקיפין, ב-50% או יותר מכל סוג של אמצעי השליטה בעסק זעיר, קטן או בינוני". "אמצעי שליטה" לעניין זה – כהגדרתו בחוק הבנקאות (רישוי), התשמ"א-1981.

ההצעה אינה של חברת בת של עסק גדול. "עסק גדול" לעניין זה: "עוסק מורשה או מוסד כספי, כהגדרתם בחוק מס ערך מוסף, התשל"ו-1975, המעסיק יותר מ-100 עובדים או שמחזור העסקאות השנתי שלו עולה על 100 מיליון שקלים חדשים".

13.4. הכרה בנתונים של אישיות משפטית אחרת

13.4.1. במקרה בו בעברו של המציע התרחש שינוי ארגוני (לדוג' רכישת פעילות, התאגדות כחברה, רה-ארגון או איחוד של חברות בדרך אחרת), באופן בו הפעילות הרלוונטית בנושא המכרז השתלבה אצל המציע, יוכל המציע לבקש מהמזמין בכתב ובאופן מנומק לצרף לנתוניו את נתוני הגוף בו התקיימה הפעילות לפני השינוי הארגוני לשם הכרה בעמידה בתנאי סף מקצועי, אחד או יותר, או בתנאים אחרים הקבועים במכרז, או לשם קבלת ניקוד איכות והכל בכפוף לכללים הקבועים במכרז.

13.4.2. אם המציע מבקש שיכירו לו בנתונים של אישיות משפטית שונה לצורך עמידה בתנאי הסף מסוים או מספר תנאי סף או לשם קבלת ניקוד איכות, בהתאם לתנאים המפורטים במכרז, עליו לפרט את כלל הפרטים הרלוונטיים

לצורך הכרה כאמור, ולצרף כל מסמך שיכול להוכיח על השינוי המבני, ועל השתלבות הפעילות הרלוונטית אצלו.

13.4.3. החלטה בדבר הכרה כאמור תהיה בכפוף לשיקול דעת המזמין.

13.5. **בקשה לחיסיון**

13.5.1. בהתאם למפורט בפרק א' למסמכי המכרז, להלן העמודים, הסעיפים או המסמכים הכלולים בהצעה אשר המציע מבקש למנוע ממציעים אחרים במכרז לעיין בהם (בטענה לחשיפת סוד מסחרי או סוד מקצועי או כל נימוק אחר המופיע בתקנה 21(ה) לתקנות חובת המכרזים):

מספר עמוד/סעיף	נושא הסעיף	נימוק למניעת החשיפה

<u>אישור והתחייבות</u>

בחתימתנו אנו מאשרים כי:

1. **קראנו את כל הוראות המכרז, והצעתנו מוגשת בהתאם לכללי המכרז ועומדת בתנאים ובדרישות המפורטות במסמכי המכרז.**
2. **כל סעיף במכרז מובן ומקובל עלינו, והמציע יהיה מנוע ומושתק מלהעלות טענות כנגד תנאי המכרז מרגע הגשת הצעה זו.**
3. **הפרטים המופיעים בהצעה זו על נספחיה, הם אמת, וכי המציע מסוגל ומתכוון לעמוד בכל פרט מהצעתו ובהוראות המכרז.**

_____	_____	_____
תאריך	שם	חתימת מורשה החתימה
_____	_____	_____
תאריך	שם	חתימתה מורשה החתימה
_____	_____	_____
תאריך	שם	חתימת מורשה החתימה

14. רשימת נספחים

מס' נספח	שם נספח	תיאור נספח
נספח 1	**הצעת מחיר**	טופס הצעת מחיר מלא בהתאם להוראות המופיעות בנספח.
נספח 2	**אישור "פקיד מורשה"**	על המציע לצרף אישור תקף מרואה חשבון או מיועץ מס על ניהול פנקסי חשבונות, ודיווח לרשויות המס כנדרש בחוק עסקאות גופים ציבוריים, או אישור על פטור מחובה זו. לצורך כך ניתן להשתמש בקישור הבא: https://www.misim.gov.il/gmishurim/frmInputMekabel.aspx?cur=0
נספח 3	**תצהיר עו"ד בדבר היעדר הרשעות בהתאם לחוק עסקאות גופים ציבוריים**	על המציע לצרף תצהיר עו"ד בהתאם למפורט בנספח.
נספח 4	**תצהיר מידע פלילי**	על המציע לצרף תצהיר זה עבור כל גורם שנדרש במסגרת המכרז.

נספח 1 – טופס הצעת המחיר למכרז 11/2026-אפיון, הקמה והתפעול של מרכז ניטור ותגובה סייבר במגזר התחבורה (TSOC)

טופס זה יוגש בנפרד מחוברת ההצעה

<u>כללי</u>

1. על המציע לעיין בכלל מסמכי המכרז טרם מילוי טופס הצעת המחיר.
2. מובהר, כי המשקלים המפורטים ביחס ליחידות התמחור מטה, הם בבחינת הערכה בלבד לשם חישוב ההצעה הזוכה ואין לראות בהם משום ביטוי או שיקוף כלשהו לכמויות שיוזמנו מהספק במסגרת ההתקשרות. למזמין מסור שיקול הדעת המלא והבלעדי לקבוע את היקף השירותים שיוזמנו לפי צרכיו בפועל.

<u>הצעת המחיר</u>

1. כל שורה בטבלה מהווה יחידת תמחור נפרדת. יש להקפיד למלא את כל יחידות התמחור ולעשות כן, בהתאם לכללים המופיעים תחת הטבלה.
2. ניתן לנקוב במחיר הכולל עד שתי ספרות לאחר הנקודה העשרונית. מובהר, כי ככל שהמציע יציין יותר משתי ספרות לאחר הנקודה, הסכום יעוגל כלפי מטה כך שיילקחו בחשבון רק שתי הספרות הראשונות לאחר הנקודה העשרונית.
3. יש למלא רק את העמודה המסומנת "למילוי על ידי המציע".

טבלה 1 - הצעה כספית

מס.	יחידת התמחור	מטבע	מחיר מינימום	מחיר מקסימום	משקל	הצעת המחיר - למילוי ע"י המציע (כולל מע"מ)
1	עלות הקמה - עלות עבור שלבים א'-ג' (עלות כוללת)	שקל	ללא	4.2 מש"ח	20%	₪
2	עלות עבור שלב ד' (לתקופה כוללת של 17 חודשים)	שקל	9.5 מש"ח	13 מש"ח	65%	₪
4	**אופציה -** רישוי והפקת מערכות מודיעין מסחרי באופן שיכסה הכלת 50 גופים	שקל	ללא	1 מש"ח	2%	₪
5	**אופציה -** רישוי והפקת מערכת לסריקת חולשות באופן שיכסה 50 גופים	שקל	ללא	0.7מש"ח	1%	₪
6	**IR - שעה הרחבה על פי דרישה**	שקל	300 ₪	700 ש"ח	6%	₪

7	**צוות אינטגרציה - שעה הרחבה על פי תמחור**	שקל	250 ₪	450 ש"ח	6%	₪

כללים נוספים עבור טבלה זו:

1. תקופת ההפעלה (שלב ד') נכנס לפעולה בסיום ואישור שלב ג' בלבד.
2. עבור מרכיב העלות בשורה 2, יש לחלקו ל 17 חודשי הפעלה ולפרט את מרכיבי העלות החודשיים בטבלה 2 מטה.
3. עלות ההפעלה החודשית (בהתאם לפירוט בטבלה 2) תהווה גם העלות החודשית להמשך התקשרות (הפעלת אופציה שלאחר סיום 24 חודשי ההתקשרות).
4. המחיר המוצע עבור סעיף 2 יכללו מרכיב שינויים ושיפורים בגובה של 2% מימוש סעיף זה יהיה בכפוף לאישור סגן חשב המשרד.
5. לא יושתו עלויות נוספות על המשרד מעבר לעלות ההפעלה החודשית (במידה והספק יידרש לתגבור כ"א בנקודות עומס מסויימות או אם לאור תקלה מסויימת EPS/נפחי המידע יקפצו – התשלום החודשי לא ישתנה).
6. במידה ולא יוצע מחיר לגבי אחת או יותר מיחידות התמחור לעיל, ההצעה כולה תפסל ותדחה על הסף.
7. על הסכומים המוצעים להיות סופיים ולכלול כל מס, ובכלל זה מע"מ כשיעורו על פי דין (ככל שהמציע חב בתשלום מע"מ). יודגש כי מציע אשר בהתאם להוראות הדין אינו מחויב בתשלום מע"מ במסגרת ביצוע ההתקשרות, יציין זאת באופן מפורש וברור במסגרת הצעתו.

פירוט תשלום בגין שירותי ההפעלה חודשי:

טבלה 2 - פירוט עלות הפעלה חודשי (הספק רשאי להרחיב שורות בהתאם לשיקול דעתו ובתנאי שנתן מענה לפחות לשורות הכתובת המצוינות בטבלה זו).

	מרכיב	סוג	הצעת המחיר - למילוי ע"י המציע (כולל מע"מ) **לחודש הפעלה**
א	עלויות כ"א	מנהל\ת TSOC	
		אנליסט T3	
		אנליסט T2	
		אנליסט \ בקר T1	
		איש תשתיות ואינטגרציה	
		מנהל\ת פורטל ותוכן	
ב	עלויות תשתיות	רישוי SIEM	
		רישוי SOAR	
		רישוי Ticketing	
		סביבת הענן	
		רישוי Big Data	
ג	ניצול בנק שעות	שעות צוות IR	
		שעות צוות תשתיות ואינטגרציה	

התמורה החודשית תחושב בהתאם לקיבולת הגופים עד ליישום הניטור על פני 50 הגופים במגזר התחבורה באופן הבא:

עלות הפעלת המרכז בקיבולת גופים בהתאם	עד 20 גופים (כולל) – 80% מחודש הפעלה
	מעל 20 ועד 30 גופים (כולל)- 85% מחודש הפעלה
	מעל 30 ועד 40 גופים (כולל)- 90% מחודש הפעלה
	מעל 40 ועד 50 גופים (כולל)- 100% מחודש הפעלה

כמות הגופים לניטור ותוכנית החיבורים תוגדר ותאושר ע"י המזמין.

<u>חבות במע"מ – למילוי רק על ידי מציע שאינו חב במע"מ על פי דין במסגרת ההתקשרות</u>

1. מציע שאינו חב בתשלום מע"מ במסגרת ביצוע התקשרות זו על פי דין, יצהיר על כך כלהלן (יש לסמן X במקום המתאים):

☐ המציע מצהיר כי במסגרת התקשרות לפי מכרז זה, אם יזכה, לא יהיה חייב בתשלום מע"מ וכי הוא פנה לרשות המיסים לקבלת אישור על כך.

<u>המציע מתחייב כי:</u>

1. לאחר שעיין במסמכי המכרז על כל נספחיו לרבות נוסח ההסכם ונספחיו, המציע מגיש בזאת הצעת מחיר למכרז.
2. מעבר למפורט בנספח זה לא יידרש על ידי המציע כל סכום נוסף אלא אם נכתב אחרת באופן מפורש במקום אחר במסמכי המכרז.
3. המציע אינו מתנה הצעה זו בשום תנאי.

---------- ----------

חותמת המציע וחתימת מורשה חתימה של המציע

תאריך

נספח 3 – תצהיר בדבר היעדר הרשעות לפי חוק עסקאות גופים ציבוריים

1. אני הח"מ _____ ת"ז _____ לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

1.1. הנני נותן תצהיר זה בשם _____ שהוא המציע (להלן: "**המציע**") המבקש להתקשר עם עורך מכרז אפיון, הקמה והתפעול של מרכז ניטור ותגובה סייבר במגזר התחבורה (TSOC), מספר 11/2026 עבור משרד התחבורה. אני מצהיר/ה כי הנני מוסמך/ת לתת תצהיר זה בשם המציע.

1.2. בתצהירי זה, משמעותו של המונח "**בעל זיקה**" כהגדרתו בחוק עסקאות גופים ציבוריים התשל"ו-1976 (להלן: "**חוק עסקאות גופים ציבוריים**"). אני מאשר/ת כי הוסברה לי משמעותו של מונח זה וכי אני מבין/ה אותו.

1.3. משמעותו של המונח "**עבירה**" – עבירה לפי חוק עובדים זרים (איסור העסקה שלא כדין והבטחת תנאים הוגנים), התשנ"א-1991 או לפי חוק שכר מינימום התשמ"ז-1987, ולעניין עסקאות לקבלת שירות כהגדרתו בסעיף 2 לחוק להגברת האכיפה של דיני העבודה, התשע"ב-2011, גם עבירה על הוראות החיקוקים המנויות בתוספת השלישית לאותו חוק.

1.4. המציע הינו תאגיד הרשום בישראל. (סמן X במשבצת המתאימה):

☐ המציע ובעל זיקה אליו לא הורשעו ביותר משתי עבירות עד למועד האחרון להגשת ההצעות (להלן: "מועד להגשה") למכרז אפיון, הקמה והתפעול של מרכז ניטור ותגובה סייבר במגזר התחבורה (TSOC), מספר 11/2026.

☐ המציע או בעל זיקה אליו הורשעו בפסק דין ביותר משתי עבירות וחלפה שנה אחת לפחות ממועד ההרשעה האחרונה ועד למועד ההגשה.

☐ המציע או בעל זיקה אליו הורשעו בפסק דין ביותר משתי עבירות ולא חלפה שנה אחת לפחות ממועד ההרשעה האחרונה ועד למועד ההגשה.

זה שמי, להלן חתימתי ותוכן תצהירי דלעיל אמת.

_____ _____ _____

תאריך שם חתימה וחותמת

<u>אישור עורך הדין</u>

אני הח"מ _____, עו"ד מאשר/ת כי ביום _____ הופיע/ה בפני במשרדי אשר ברחוב _____ בישוב/עיר _____ מר/גב' _____ שזיהה/תה עצמו/ה על ידי ת"ז _____ /המוכר/ת לי באופן אישי, ואחרי שהזהרתיו/ה כי עליו/ה להצהיר אמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, חתם/ה בפני על התצהיר דלעיל.

_____ _____ _____

תאריך מספר רישיון חתימה וחותמת

נספח 4 – מידע פלילי

(יש להגיש תצהיר זה על ידי כל גורם אשר בהתאם להוראות המכרז נדרש בעניינו מידע פלילי)

אני הח"מ _____ ת"ז _____, מצהיר/ה בזה כדלקמן:

1. הנני נותן תצהיר זה במסגרת הצעת _____, תאגיד הרשום/ע.מ. בישראל, שהוא המציע (להלן: "**המציע**") במכרז מספר 11/2026 לאפיון, הקמה והתפעול של מרכז ניטור ותגובה סייבר במגזר התחבורה (TSOC), ובכפוף להוראות חוק המידע הפלילי ותקנת השבים, תשע"ט-2019 (להלן: "**חוק המידע הפלילי**").

2. אחת החלופות הבאות מתקיימת בענייני:

2.1. אין כנגדי רישום פלילי במרשם הפלילי או במרשם המשטרתי אשר טרם התיישנה או נמחקה בעבירות, אחת או יותר, לפי החוקים המנויים להלן:

2.1.1. עבירות גניבה – סעיפים 290 עד 297 לחוק העונשין, התשל"ז-1977 (להלן: "**חוק העונשין**").

2.1.2. עבירות מרמה – סעיפים 414 עד 438 לחוק העונשין.

2.2. יש כנגדי רישום פלילי כאמור בסעיף (ב)(1) לעיל, אולם אין במידע זה כדי למנוע מהמציע לספק ולבצע את ההתקשרות נשוא המכרז, מהסיבות המפורטות להלן:

_____
_____
_____
_____
_____

3. אני הח"מ נותן/ת בזה את הסכמתי לכך שמשטרת ישראל תמסור מידע עליי מהמרשם הפלילי, וכן מידע על תיקים תלויים ועומדים, בהתאם להוראות חוק המידע הפלילי לוועדת המכרזים של משרד התחבורה, לשם התמודדות של המציע במכרז האמור לעיל לפי סעיף 14 לחוק המידע הפלילי. יובהר כי הסכמתי זו חלה גם על מסירת מידע פלילי לגורם הנ"ל מזמן לזמן לשם מעקב תקופתי אחר שינויים שחלו במידע הפלילי עליי.

4. הובא לידיעתי כי אני זכאי לפי החוק לעיין בתחנת משטרה ברישומים המנוהלים על שמי במרשם הפלילי ובמרשם המשטרתי.

5. הובהר לי בזה כי אם יש לחובתי רישום כאמור, אין בכך בהכרח כדי לשלול את קבלת הזכות או התפקיד ואני רשאי/ת לצרף מידע על שיקומי או נסיבותיי האישיות כדי שיילקח בחשבון בעת בחינת בקשתי, בהתאם לאמות המידה שנקבעו בחוק[1].

6. ידוע לי כי בהסכמתי זו, אני מוותר/ת על קבלת הודעה על מסירת המידע, וכל זאת בכפוף להוראות החוק.

[1] לעניין תאגיד, שיקום ייבחן, בין היתר, באימוץ אמצעי ציות, בקרה ואכיפה אפקטיביים.

זה שמי, להלן חתימתי ותוכן תצהירי דלעיל אמת.

_____

תאריך	שם	חתימה (וחותמת)

פרק ג' – פירוט השירותים ותוכן ההתקשרות עם הספק הזוכה

חלק 1 – חלק מקצועי (מפרט)
מכרז 11/2026 לאפיון , הקמה ותפעול מרכז ניטור אבטחת סייבר (TSOC) למגזר התחבורה עבור אגף חירום, בטחון, מידע וסייבר במשרד התחבורה

סיווג רכיבי המפרט

רכיבי המפרט מסווגים לפי הסימון הבא:

- **I (Information)** – רכיב לידיעה בלבד. יש לענות עליו: "קראנו והבנו, מקובל עלינו". אם יש הערות או הסתייגויות חובה לציין אותן.
- **G (General)** – רכיב הדורש תשובה כללית ובפורמט יחסית חופשי. בד"כ זהו סעיף "פתוח" בו ניתן להוסיף הצעות ופתרונות יצירתיים, ובלבד שבסופו של דבר יינתן מענה ברור לדרישה, יודגשו התכונות העיקריות ויהיה ברור מה בדיוק מוצע, מה כבר קיים ומה מובטח \ מוצע שיהיה.
- **S (Specific)** – רכיב הדורש תשובה מפורטת ומדויקת, בפורמט מדויק שנדרש במפרט: מילוי טבלה, צירוף אישורים וכו'. בד"כ זהו סעיף "סגור". ניתן להוסיף מידע מעבר לנדרש בכפוף להנחיות שבסיווג G. אם המידע רב, יש להוסיפו כנספח בסימון המתאים.
- **M (Mandatory)** – רכיב סף (Go/NoGo), נקרא גם סעיף חובה (Mandatory). (ה"חובה" היא בתוכן הסעיף ולא בעצם הצורך לענות. הצורך לענות חל על כל סעיפי המפרט כמוסבר בחלק 0 להלן). תשובת המציע תהיה מסוג "קראנו והבנו - מקובל עלינו, הצעתנו עונה על דרישות סעיף זה", או תשובה ענייינית ומלאה בדומה לסיווג S, או קיום דרישה (המצאת אישור למשל) או התחייבות לקיום דרישה הכל בהתאם לענייננו ותוכנו של הסעיף. חוסר תשובה, תשובה שאיננה עונה לדרישה, חוסר מענה לדרישה, או תשובה לא ברורה ולא חד משמעית, בסעיף מסוג זה, תפסול את ההצעה על הסף.

סיווג רכיב אב תקף לכל הבנים, אלא אם צוין ברכיב הבן אחרת. כלומר: רכיב שמסומן לידו סיווג - זה הסיווג המחייב. רכיב שאין לידו סימון - יש לקחת את סיווג רכיב האב שלו.

מעבר לכל סיווג יש לשים לב להנחיות שבגוף הסעיף ולדרישות המנוסחות שם.

הצעת המציע

מבנה כללי

מבנה ההצעה יהיה תואם אחד לאחד 1:1 למבנה המפרט. לדוגמא: סעיף 2.1 בהצעה יכיל תשובה לרכיב 2.1 במפרט, סעיף 2.2 תשובה לרכיב 2.2 וכו'.

למען הסר ספק מובהר בזאת כי התשובות תינתנה בהתאמה 1:1 גם לתת חלוקה של כל סעיף, לכל רמת פירוט שהיא.

רכיב לגביו אין תשובה ייכתב לידו "אין תשובה" והרכיב הבא אחריו ישמור על מספרו המקורי במפרט.

מבנה מפורט

- תוכן ומבנה התשובה בכל רכיב (ותת-רכיב) יתאים לסיווג הרכיב: G, I, M או S, כמוגדר לעיל .
- ברכיבים המסומנים G, יש להדגיש אם קיים או לא קיים ולציין תכונות חשובות בלבד, בקצרה ובמלל חופשי (עד 1/2 עמוד לרכיב)
- ברכיבים המסומנים S, יש לספק תשובה מפורטת כולל תעתיקים ממערכות אחרות או מתיעוד קיים ובלבד שתהיה תשובה ברורה לדרישה המתאימה.
- **המשרד מדגיש את חשיבות פירוט ארכיטקטורת הפתרון המוצע במסגרת האפיון הראשוני (במסגרת המענה למכרז) לפרטים, לרבות התקנות רכיבים בצד הגופים, איסוף המידע מהם, תצורת החיבור אליהם ומענה ההגנה. לפירוט זה משקל מהותי ביכולת המשרד להבין ולנקד את ההצעות** .
- במקרה של תשובה ארוכה יש להפנות לנספח בסוף ההצעה. חשוב להשתמש בנספחים על מנת לפשט את גוף ההצעה ולהקל על קריאתה. חומר מקצועי ופרסומי יצורף כנספח לסעיף הרלבנטי ויסומן כמפורט לעיל.
- יש להבחין בין רכיב "סגור" הדורש תשובה של "כן / לא" או מילוי טבלה מוגדרת, לבין רכיב "פתוח" המאפשר תשובה במבנה חופשי.
- ברכיב "פתוח", רשאי המציע להוסיף הערות והצעות משלו ע"י הוספת סעיף "אחר". סעיף זה יסומן X.97 בסוף רכיב ראשי, או X.Y.97 בסוף רכיב משני

<u>סיווג החלק המקצועי (חלק 1)</u>

סיווג רכיבי החלק המקצועי (חלק זה) מצוין בגוף המפרט ליד כותרתו של כל סעיף (או ברכיב האב שלו). מעבר לכל סיווג יש לשים לב להנחיות בגוף הסעיף ולדרישות המנוסחות שם.

<u>בעלות על המפרט ועל ההצעה (M)</u>

- מפרט זה הוא קנינו הרוחני של משרד התחבורה אשר מועבר למציע לצורך הגשת הצעה בלבד. אין לעשות בו כל שימוש שאינו לצורך הכנת ההצעה.
- הצעת המציע (המענה בקשה להצעת מחיר) היא רכושו של המציע. למשרד התחבורה תהא האפשרות להשתמש בהצעה ובמידע שבה לכל צורך הקשור בתהליך זה של בקשה להצעות עד להשלמת הפעילות במכרז זה והתקשרות עם המציע.

המשרד מתחייב שלא לגלות תוכן ההצעה לצד שלישי זולת ליועצים המועסקים על ידו אשר גם עליהם תחול חובת הסודיות ואי השימוש בהצעת המציע אלא לצורכי הפרויקט בלבד.

- בהתאם לתקנה 21 (ה) לתקנות חובת המכרזים, התשנ"ג – 1993, עומדת למציעים שלא זכו במכרז, הזכות לעיין בהצעה הזוכה. המציע מתבקש לסמן באופן בולט את החלקים בהצעתו, המהווים לדעתו מידע סודי מסחרי שאין לגלותו.(נספח ז') יובהר כי ההצעה הכספית לא תהא חסויה בכל מקרה. המציע לא יהא רשאי לקבל מוועדת המכרזים פרטים על אודות הצעות של מציעים אחרים, החופפים את אלו שסומנו על ידו כמידע סודי ואסור לפרסום .
- החלקים שלא סומנו כמידע חסוי, ייחשבו כמידע הניתן לגילוי במידת הצורך, לרבות העברתם לעיון מציעים שלא זכו במכרז.
- מובהר, כי ההחלטה הסופית לגבי חלקי ההצעה הניתנים לפרסום, ככל שיידרש, תתקבל על ידי ועדת המכרזים בלבד, וועדת המכרזים תהיה רשאית, עפ"י שיקול דעתה, להציג בפני המתחרים שלא זכו במכרז, כל מסמך אשר להערכתה המקצועית אינו מהווה סוד מסחרי או מקצועי.
- המשרד מבהיר כי מבקר הפנים של המשרד רשאי בכל עת לקבל כל מידע שידרוש מהספק עפ"י שיקוליו ולקיים ביקורת מקצועית והספק חייב להיענות באופן מידי ומלא לדרישות המבקר.

<u>שינויים בדרישות (M)</u>

- על הספק להיות מודע לכך ולקחת בחשבון כי יצטרך לבצע במהלך העסקתו התאמות, שינויים ושיפורים לפי דרישות המשרד. תמחור השינויים הם רכיב כולל במדד המחיר במכרז.
- היקף המערכות המתוארות מבחינת כמות שרתים ו/או כמות יישומים, כמפורט בחלק המקצועי הינם הערכה בלבד. שינויים בכמויות אלה, הנובעים מתוצאות סקר המצב הקיים ו/או מהתפתחות טכנולוגית שתהיה במהלך שנות הפרויקט לא יחשבו כשינויים.
- שינויים, תוספות לדרישות וגריעות מהדרישות ימסרו לספק בכתב. הספק ישיב לדרישת הערכת עלות ולו"ז חדש, בכתב. הספק יבצע השינוי רק לאחר קבלת אישור בכתב מהמשרד.
- במהלך תקופת ההתקשרות, אם יחולו שינויים טכנולוגיים מהותיים בשוק, לרבות הופעת פתרונות מתקדמים או סטנדרטים חדשים בשוק מערכות ניטור ואבטחת סייבר, שיאומצו באופן נרחב או שיוגדרו כפתרונות מומלצים ע"י גורמים מוסמכים (רגולציה ממשלתית ישראלית/בינלאומית, חברות כגון גרטנר ועוד), שומר לעצמו המזמין את הזכות לדרוש מהספק הזוכה להציע תוכנית להטמעת טכנולוגיות אלו במחירי עלות בתוספת עד 5% עלות תקורות רכש. כל שינוי כאמור יתואם מראש, בכפוף לשיקול דעתו של המזמין ובאישור חשב המשרד.

<u>שלמות ההצעה ואחריות כוללת (M)</u>

- המציע יגיש הצעה אחת כוללת (כולל התייחסות להתקנות המערכות במרכז ובצד הג"מים).
- המציע יהיה אחראי לאופן אספקת השירותים ואיכותם. האחריות הינה בין היתר לביצוע מקיף ומלא של השירותים כפי שיוגדרו בכתב על-ידי דרישות נציג המשרד ומי מטעמו (להלן: "נציג המשרד"). המציע/הספק יקיים את דרישות/הוראות נציג המשרד ובלבד שלא יסתרו הוראות חוזה זה.
- ככל שמדובר במוצרי צד ג' המשולבים בפתרון מבוקש, יהיה הספק אחראי לאינטגרציה של כל רכיבי המערכת כ- single point of contact בנוגע לכל תקלה בכל רכיב הפתרון, כאשר האחריות למוצרי צד ג', המשולבים בפתרון, ולתחזוקת מוצרי התוכנה של צד ג', הנה של הספק בהתאם לרישיון התוכנה ו/או תעודת האחריות, לפי העניין.
- על המציע לצרף להצעתו תמצית מנהלים.

1. יעדים (I)

1.1. כללי

1.1.1. המשרד מעוניין לקבל הצעות לאפיון הקמה ותפעול מרכז ניטור אבטחת סייבר (TSOC) להגנת מפני איומי סייבר על תשתיות ממשלתיות ואזרחיות חיוניות במגזר התחברה. כחלק מהמענה יכין הזוכה אפיון מפורט על פי התוכנית שתוגדר על ידי המשרד. האפיון יבוצע בתאום ובשיתוף מלא עם מנהל הפרויקט וצוות ייעודי, שהמשרד ימנה לליווי האפיון המפורט.

1.2. לקוחות ה-TSOC

1.2.1. לקוח \ משתמש עיקרי

המשרד – יחידת הסייבר המגזרית, לרבות מקבלי החלטות בדרגים שונים בהנהלת משרד התחבורה, הגופים המנוטרים לרבות הSOC-ים אותם הם מפעילים. מערך הסייבר בהיבט תמונת מצב מגזרית המתגבשת וה SOC לאומי. החוקרים עצמם ,וצוותיIR .

1.2.2. לקוחות נוספים

גופיים מנוטרים במגזר התחבורה, מערך הסייבר הלאומי, מרכזים מגזריים נוספים, גופים ממשלתיים אחרים וגופים אחרים לפי הגדרת המשרד .

1.3. יעדים ומטרות (G)

1.3.1. יעדים כלליים

מרכז לגיבוש תמונת מצב מגזרית בסייבר בגופים מנוטרים (להלן ג"מ) מתועדפים על ידי היחידה המגזרית בסייבר של משרד התחבורה. המרכז יפעל לאיתור ולהתראה על פעילות טכנולוגית חשודה אל מול הג"מים, ויצירת תשתית איתורית-מחקרית כבסיס לסיוע באירועים בגופים, לחיזוק חוסנם, תוך אחזקת תמונת איומים טכנולוגיים רציפה ומתעדכנת. שיתוף מידע וידע על אירועי סייבר בין גופי המגזר, העלאת/הורדת רמות כוננות של המגזר, החזקת תמונת מצב כוללת בזמן אמת, עדכנית ומקיפה של מפת האיומים, התקפות סייבר ואירועים אבטחתיים, יכולת זיהוי, שליטה, הכלה ותגובה של אירועי סייבר במגזר התחבורה.

1.3.2. מטרות עיקריות

מטרתו העיקרית של הפרויקט היא הקמת מרכז ניטור אבטחת סייבר מגזרי לתחבורה (TSOC) שיאפשר איתור והתרעה על איומי סייבר המסכנים את הרציפות התחבורתית במדינת ישראל, לתכלל את כלל הנושאים, הצרכים והמערכות הנדרשים לשם איסוף הנתונים, ניתוחם, שיתופם והצגתם במקום מרכזי לכדי בניית תמונת מצב אבטחת סייבר מגזרית, אחודה.

- להתריע על פערי חוסן מהותיים בג"מים.
- קבלת מזהים בזמן אמת מגופים חיצוניים (מערך הסייבר הלאומי באמצעות MISP כדוגמא) להצליב מזהים שלא ניתנים לשיתוף עם הג"מים ע"ב פלטפורמה חיצונית להם.
- לשתף במידע ולקבל מידע, מג"מים מהמגזר ומגופים לאומיים מחוץ למגזר.
- להעלות או להוריד מצבי כוננות.
- לגבש ולשקף תמונת מצב כוללת, עדכנית ומקיפה של האיומים במגזר.
- לאתר, לזהות ולהתריע על התקפות סייבר על סמך מידע מהג"מים, מידע מגורמים לאומיים מוסמכים ומקורות מודיעין מסחרי.
- לסייע לג"מים בזמן האירוע ולאחריו.
- לאפשר תחקור, ניתוח, למידה והפקת לקחים מאירועי סייבר.
- לגבש פתרונות חדשניים להגנה סייבר.
- לתמוך בהעברת הנחיות המשרד לג"מים, לטובת שליטה, הכלה ותגובה לאירועים ברמת המגזר.
- השתלבות בתמונת המצב הלאומית המיוצגת על ידי ה NSOC של מערך הסייבר הלאומי.

1.4. הקשר ארגוני \ עסקי

1.4.1. השלכות ארגון ושיטות

במסגרת הקמת המערכות יהיה צורך לגבש ממשקים אוטומטיים ונהלי עבודה סדורים למול כ-50 ג"מים מובילים ומתקדמים במגזר התחבורה, אשר מקיימים בין היתר פעילות SOC עצמאית, תוך כוונה לשלב את כלל מקורות המידע מכלל הג"מים למרכז אחוד לקבלת תמונת מצב לאומית ולהבטיח רציפות תחבורתית ולייצר תמונת מצב עדכנית המשלבת מידע אבטחתי ברמה הלאומית בשילוב מידע מכלל הג"מים תוך סיוע בטיפול באירועים מול

הגופים, בין המגזרים השונים כגון NSOC ומול מרכז ניטור אבטחת סייבר (TSOC).

1.4.2. תלות במערכות אחרות

למערכות במרכז ניטור אבטחת הסייבר (TSOC) נדרשת יכולת התממשקות עם מערכות מערך הסייבר הלאומי, מערכות מקומיות מערכות On-Prem, מערכות ענניות Cloud, מערכות תפעוליות, מערכות תקשורת מסוגים שונים, מערכות מפלטפורמות תחבורתיות מתקדמות, "אינטרנט של דברים IoT" ומערכות אבטחה ממספר רב של ארגונים ופלטפורמות מחשוב חיצוניות הקיימות במגזר ומחוץ לו. בחלק מהמקרים תידרש יכולת התממשקות אוטומטית בחלקן, ידנית ובחלקן חצי אוטומטית, הכול לפי העניין. ככלל, מרכז ה TSOC לא יהיה תלוי ב SIEM של הג"מים. ניתן יהיה לקבל תמונה משלימה ממערכות SIEM אלה, אך נדרש להסתמך על יכולת עצמאית לאיסוף המידע ממוצרי ההגנה ונכסי השליטה בגוף, ניתוח **המידע ואיתור החשדות/אירועים,** גם כאשר רכיבים מסויימים בג"מים יהיו מוגבלים בשליחת נתונים ליעד אחד (רכיב ה SIEM הארגוני).

1.4.3. הבטחת רציפות תפקוד המרכז וזמינות בעלי התפקידים במצבי חירום ומשבר

1.4.3.1. המרכז נחשב כגוף חיוני לרציפות **תפקודם** של כלל מערכי התחבורה ביום יום ובמיוחד במצבי חירום ומשבר ואמור לפעול במצבי אלו באופן מלא ואף בצורה מתוגברת

1.4.3.2. הכרזת מצב החירום יחשב אחד מאלו: בעקבות מצב החירום, הגורמים המוסמכים יכולים להכריז על: תקופת הפעלת מערך משק לשעת חירום (מל"ח) בהתאם להחלטת הממשלה מס 1716 מיום כ"ט בסיון התשמ"ו 6) ביולי ,(1986 להחלטת ממשלה מס 1080 מיום ז' באדר א התש"ס 13) בפברואר (2000 וכל החלטת ממשלה אחרת בעניין, הכרזה על מצב מיוחד בעורף לפי סעיף9 ג לחוק התגוננות אזרחית תשי"א 1951 -או הכרזה על "אסון אזרחי" כמוגדר ב"פקודת המשטרה" ו/או בהתאם לקביעת הממונה מטעם משרד התחבורה

1.4.3.3. סוגי מצבי חירום ומשבר רלוונטיים:

1.4.3.3.1. מלחמה כוללת או אירוע ביטחוני נקודתי

1.4.3.3.2. טרור קונבנציונלי וטרור בלתי קונבנציונלי(טב"ק).

1.4.3.3.3. רעידת אדמה בעוצמה משתנה ,לרבות צונאמי.

1.4.3.3.4. מגפה (פנדמיה).

1.4.3.3.5. אירוע חירום משמעותי בשגרה – אירוע המתרחש במהלך שגרה וגורם לשיבוש חיי השגרה באופן משמעותי ברמה ארצית או אזורית (דוגמא: השריפה הגדולה שהייתה ביערות הכרמל, אירוע מזג אוויר סוער, תאונות ותקלות תפעוליות, הפרות סדר, אירועי חומרים מסוכנים וכיוצא בזה).

1.4.3.3.6. אירוע חירום מקומי בשגרה – אירוע המשפיע על תפקודו השוטף של מבנה בודד כגון: הצפות, שריפה, קריסת מבנה ועוד.

1.4.3.3.7. אירועי סייבר ואבטחת מידע.

1.4.3.4. **מובהר בזאת שמצבי חירום ומשבר אשר הוגדרו לצורך רציפות תפקוד המרכז במצב חירום, לא יוכלו לשמש עילה לספק ולטעון בדבר "כוח עליון".**

1.4.3.5. על הספק לבצע ניתוח סיכונים מקיף לכלל התרחישים שעלולים לשבש את תפקוד המרכז במצבי חירום ומשבר, ולהכין תוכנית מענה מתאימה, כולל הקצאת משאבים למימושה.

1.4.3.6. על הספק למנות בעל תפקיד מטעמו, אשר יהיה אחראי על הבטחת רציפות התפקוד של המרכז במצבי חירום ומשבר

1.4.3.7. על הספק להיות ערוך לספק חלופות עבודה ידנית – הכללת נהלים לביצוע תהליכים קריטיים באופן ידני במקרה של כשל טכנולוגי

1.4.3.8. הספק מתחייב שהמידה ויידרש ע"י הממונה להיות מוכרז כ"מפעל חיוני" כהגדרתו ב[חוק שירות עבודה בשעת חירום, תשכ"ז-1967](), הוא יבצע את כל הנדרש ממנו

1.4.3.9. הספק מתחייב שהמידה ויידרש ע"י הממונה, הואיטפל בהכרזה על ריתוק משקי "של עובד חיוני – גיוס חובה של עובדים לעבודה בשעת חירום", בכפוף לצו המורה זאת מטעם משרד העבודה, ובהתאם ל[חוק שירות עבודה בשעת חירום, תשכ"ז-1967]()

1.4.3.10. על הספק לנקוט בצעדים אשר יבטיחו את זמינותם של ספקי המשנה להמשיך ולספק את הטובין ו/או השירותים החיוניים להמשך פעילותו של הספק

1.5. ישימות ועלות-תועלת

1.5.1. סיכונים - ישימות הפרויקט

1.5.1.1. במסגרת הפרויקט יש להקפיד שלאחר השלמת מימוש הפתרון בתצורת ה PILOT בשלב ה POC עבור מספר מצומצם של ג"מים – הפתרון יותקן וימומש ביתר הג"מים בהליך מזורז על בסיס הפקת לקחים ותכנון מוקפד מראש לייעול תהליכי ההטמעה.

1.5.1.2. הפתרון המוצע מתבקש להיות בתצורת ענן – נדרש לבצע תכנון מקיף של המענה תוך התחשבות בכלכלת ענן יעילה בהתאם לעקרונות FinOps תוך ביצוע בקרה, אכיפה, משילות והתייעלות קבועה ומתמשכת ליצירת אפקטיביות אופטימלית של ההצעה בהיבט הכלכלי תוך הערכת צפי עלויות עבור כל שלבי הפרויקט.

1.5.1.3. יחד עם האמור לעיל, על המענה להיות חדשני ובראיה עתידית, בדגש על קיימות (תכנון ירוק והתחשבות בסביבה).

1.6. אופק הזמן

מימוש הפרויקט יהיה בטווח של כחצי שנה ולמינימום התקשרות של 24 חודשים.

1.7. ניהול פרויקט

הספק שייבחר ינהל את עבודתו בפרויקט על פי מתודולוגיה סדורה כדוגמת זו של ארגון ה PMI. מיד לאחר קבלת ההזמנה יגיש הספק למשרד לוח זמנים סדור לניהול הפרויקט בו יצוין המועד לקבלת שאר המסמכים המכוננים הנדרשים לניהול פרויקט.

2. יישום – מטרות, דרישות וארכיטקטורת המערכת (M)

2.1. **שלב א' – אפיון מפורט מרכז ה TSOC (I)**– יצירת תפיסת הפעלה בהתאם לתיאור דרישות המכרז ובהתאם מתן מענה טכנולוגי HLD ו LLD מבוסס ענן למענה מלא בדרישות המרכז

2.1.1. **מטרות שלב א' (G)**

2.1.1.1. **<u>תפיסת הפעלה</u>** - מטרת השלב הוא יצירת תפיסת הפעלה כוללת למרכז ניטור האבטחה TSOC למגזר התחבורה - על בסיס עקרונות מכרז זה ובהתאם לתפיסות האבטחה הנהוגות במרכזי SOC המשמשים מרכזי ניטור מגזריים בארץ ובעולם.

2.1.1.2. **<u>אפיון מענה טכנולוגי</u>** - על בסיס תפיסה יוגדר מענה טכנולוגי מקיף לטובת הקמת מרכז ניטור אבטחה (TSOC) למגזר התחבורה.

2.1.1.3. **<u>שילוב בין תפיסת הפעלה למענה הטכנולוגי</u>** - מטרת תפיסת ההפעלה והמענה הטכנולוגי יהיה לבסס את אופן מתן המענה התהליכי והתשתית אשר ישמש את מרכז ניהול אבטחת סייבר (TSOC) – בקבלת, ניתוח תחקור ודיווח אירועי אבטחת מידע וסייבר בג"מים ולגבש את תמונת מצב אבטחת הסייבר המגזרית הכוללת, על מנת לאפשר קבלת החלטות, ניהול והתמודדות עם אירועי סייבר במגזר התחבורה. מטרת המרכז לקבל ולשתף מידע וידע עדכני, רלוונטי ובעל ערך מוסף משמעותי להגנה בסייבר (actionable intelligence) בין כלל הג"מים החברים במרכז מול המשרד. כל זאת באופן מאובטח, אמין ודיסקרטי שיאפשר יצירת מכפיל כוח לצורך התמודדות מיטבית כנגד כלל איומי הסייבר במגזר התחברה.

2.1.2. **דרישות השלב (S)**

2.1.2.1. **<u>כללי</u>(M)**

תפיסת ההפעלה ואפיון המענה הטכנולוגי (להלן: **הפתרון**) יביאו לידי ביטוי את כלל הדרישות:

2.1.2.1.1. תפיסת הפעלה ייחודית המשלבת הבנה עמוקה של הצרכים למרכז טכנולוגי הפועל בסביבת פלטפורמות תחבורתיות מתקדמות ובהם:

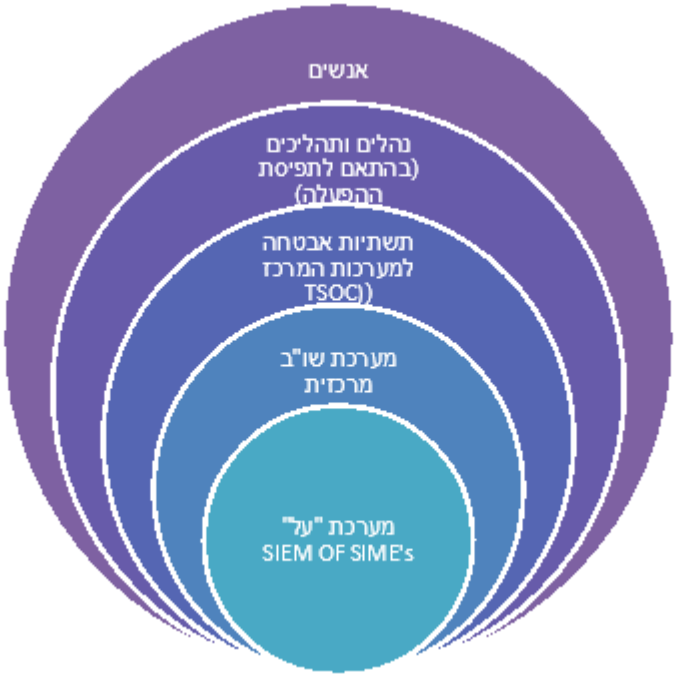
2.1.2.1.1.1. פלטפורמות יבשתיות: רכבים \ תשתיות (כבישים ורמזורים, עמדות טעינה), חברות התחברה

אוטובוסים ותחבורה מסילתית \ רכבות כבדות, קלות, רכבלים ועוד.

2.1.2.1.1.2. פלטפורמות ימיות: אוניות, נמלים, מספנות ועוד.

2.1.2.1.1.3. פלטפורמות תעופתיות: נמלי תעופה, חברות תעופה, מערכות ופלטפורמות תעופה בלתי מאוישות או מאוישות מרחוק (רחפנים) מרכזי שילוח ועוד.

2.1.2.1.2. הפתרון יתבסס על מספר מעגלים:



2.1.2.1.3. הפתרון יאפשר העברת מידע רגיש בין הג"מים לבין המשרד ומהמשרד לג"מים באופן שיאפשר גיבוש תמונת מצב עדכנית לאירועי אבטחת מידע וסייבר המתקיימים במגזר.

2.1.2.1.4. הפתרון יאפשר קבלת מידע באופן מאובטח ומוצפן למערכות מרכז ה TSOC על גבי רשת האינטרנט מכלל הג"מים וממקורות מידע נוספים.

2.1.2.1.5. הפתרון לכניסת מידע למערכות הליבה של מרכז ה TSOC יהיה בתצורה של מידע נכנס באופן חד כיווני לוגי למרכז ולא יוצא (למעט ממשקים מוגדרים מראש).

2.1.2.1.6. הגישה למערכות מרכז ה-TSOC תהיה למורשים בלבד לאחר עמידה בכלל דרישות אבטחת המידע – לא

תתאפשר כל גישה לגורמים חיצוניים למידע או למערכות ה TSOC.

2.1.2.1.7. הפתרון המוצע יהיה ייעודי למשרד התחבורה ומופרד מכל מידע או תשתית של גורמים אחרים מחוץ למשרד התחבורה.

2.1.2.1.8. הספק יבחן את מצרף המידע המעובד ונאגר בסביבה שתוקם, והאם נדרשת הגדרתו כ"מאגר מידע". במידה ויוגדר כ"מאגר מידע" יוגדר אחראי/DPO.

2.1.2.1.9. המידור ושיתוף המידע המאובטח במערכת מרכז ה TSOC יתבצע בסטנדרט גבוה כפי שמקובל על הגופים המובילים בעולם בהתאם לסטנדרטים ותקנים מובילים שיוצג במסגרת מענה.

2.1.2.1.10. המידע שיגיע באופן מאובטח למרכז ה TSOC ממקורות חיצוניים (שלא כחלק מפתרון העברת ההתראות מהג"מים) יעבור בדיקה במערכות לזיהוי קוד זדוני טרם כניסה למערכות.

2.1.2.1.11. הפתרון הטכנולוגי יבוסס על פתרונות ענן – CLOUD כאשר ספק הענן יהיה חברת BIG-TECH מערבית (AWS או GCP) תואמת למכרז הענן הממשלתי "נימבוס" המקיימות מרכז מידע בארץ ומאפשרות את שירות הפתרון מגבולות מדינת ישראל ליצירת משילות ישראלית על המידע בפתרון. הספק יוגדר כספק צד ג' בפרויקט נימבוס.

2.1.2.1.12. הפתרון הטכנולוגי יבוסס על מערכות SAAS או IAAS כאשר העדפה תהיה למימוש ומיצוי פתרונות NATIVE (לא מחייב) בדגש על שמירת המידע באזור משילות מדינת ישראל.

2.1.2.1.13. הפתרון הטכנולוגי יכלול הטמעת ותפעול יכולות AI מתקדמות לשם קיצור משך הטיפול באירועים ל"זמן מכונה", צמצום ה-FP וייעול עבודת צוות הבקרים ואחיזת תמונת פגיעויות עדכנית לרבות חוקים לאיתור נסיונות

ניצול חולשות בסמיכות גבוהה לרגע פרסומן. הפתרון יכלול בין היתר:

2.1.2.1.13.1. **חקירה וניהול אירועים מבוססי סוכני בינה מלאכותית (Cyber Agents & AI Analyst)** המערכת תשלב "סוכני סייבר" ומנועי AI לאוטומציה של איסוף נתונים, סינון התראות שווא (False Positives) וקיבוץ אירועים (Alert Clustering) במטרה לקצר משמעותית את זמני התגובה (MTTD/MTTR) ולהפחית את העומס על האנליסטים האנושיים.

2.1.2.1.13.2. **ניהול חשיפות וחוסן (Passive CTEM, SBOM & Posture)** הפלטפורמה תסתמך על אינטגרציות (ממשקי API, לוגים ו-MCP בגופים המנוטרים) שיאפשרו זיהוי מלאי הנכסים, התשתיות ורכיבי צד ג' (שרשרת אספקה ו-SBOM). מנועי הפלטפורמה יצליבו מידע זה אוטומטית מול מודיעין גלוי (OSINT) לשם חישוב "מדד חוסן דינמי" לכל גוף שיאופיין במשותף. יודגש כי הפלטפורמה לא תבצע סריקות חדירה אקטיביות ברשתות הגופים המונחים.

2.1.2.1.13.3. **פונקציית תפעול חולשות והנדסת גילוי מגזרית (Detection Engineering & Sectorial VulnOps)** כהיערכות לקצב גילוי החולשות המואץ, הספק ימסד תהליכים תפעוליים ייעודיים (VulnOps מגזרי) הפועלים תחת יעדי SLA מחמירים לזמן תגובה. התהליכים תמקדו במיפוי ושיקוף פגיעויות לגופים, הפצת המלצות אופרטיביות ל"חיסון" והקשחה לצוותים בגופים המונחים, כתיבה והטמעה מהירה של חוקי זיהוי (Detection Rules) ב-SOC המגזרי, ובניית תרחישי תגובה אוטומטיים (Playbooks) במערכת ה-SOAR.

2.1.2.1.13.4. **ארכיטקטורת AI/LLM ריבונית ומאובטחת (Sovereign Closed AI Environment)** כלל יכולות הבינה המלאכותית ומודלי השפה (LLM) שיוטמעו ב-SOC יבוססו על גבי תשתית ייעודית ומבודדת בתוך ה- Landing Zone בנימבוס אשר תאושר ע"י המשרד. באחריות הספק ליישם בקרות מחמירות (VPC Service Controls) המונעות הרמטית גישה לאינטרנט ופניות API's חיצוניות.
חל איסור מוחלט על הוצאת מידע, לוגים, נתוני גרסאות, או כל פריט מידע מזהה (PII/Technical Data) של הגופים המונחים אל מחוץ לסביבה המאובטחת של ה-SOC המגזרי(לרבות איסור

פנייה ל-APIs ציבוריים/מסחריים). כלל עיבוד הנתונים, מערכות ה-RAG ומודלי ה-Fine-tuning יבוצעו באופן מקומי תוך הבטחת מידור מוחלט בין נתוני הגופים השונים.

2.1.2.1.13.5. **משילות, נראות מגזרית ואינטגרציה לאומית (Governance & National Visibility)** פלטפורמת ה-SOC תייצר תמונת נראות רוחבית של המגזר כולו, ותקיים סנכרון רציף (בממשק API) מול מערכות מערך הסייבר הלאומי להעברת התרעות ופרישת חתימות רוחביות. כלל מנועי ה-AI יפעלו תחת עקרונות של שקיפות מודלים (Explainable AI) ויחייבו ניהול אנושי בתהליך (Human-in-the-loop) המצריך אישור מצוות מיומן טרם ביצוע פעולות בלימה שעשויות להשפיע על הרציפות התפקודית התחבורתית.

2.1.2.1.14. הפתרון הטכנולוגי ייקח חשבון את עקרונות FinOps "כלכלת ענן חכמה" ותבוסס על עקרון ה-Opex תוך יצירת ניהול משאבים הדוק עבור כל הפרויקט ותתי המרכיבים במטרה ליעילות כלכלית מקסימלית ושקיפות מלאה וקלה למקבלי ההחלטות – יוצג תחשיב עלויות מוערך על בסיס ההצעה לשנים 0-1 ולשנים 1-3.

2.1.2.1.15. למען הסר ספק – הספק לא יהא זכאי לתעריפים ממשלתיים ברכש ציוד.

2.1.2.1.16. הפתרון הטכנולוגי ישמור על עקרון משילות המידע לנהוג במשרדי ממשלה במדינת ישראל.

2.1.2.1.17. יש לפרט ארכיטקטורה מקיפה של הפתרון, המערכות התומכות בפתרון ושל מוצרים הכלולים בו לרבות מענה ההגנה על הסביבה עצמה (מהניטור בגוף ועד המרכז):

2.1.2.1.17.1. דרך איסוף ושינוע מאובטח של המידע אל מערכת ה"על" Siem of Siem's של מרכז ניטור אבטחת הסייבר (TSOC), מקורות המידע, שיטות האיסוף הכוללות פתרון ייעודי שיותקן בגוף המנוטר (נדרש לפרט בהתאם)

2.1.2.1.17.2. מערכות השו"ב המרכזית –אינטגרציה פנימית בין מערכות ותשתית אגירה לטווח ארוך של אירועים המאפשר אנליזות מורכבות מעל נפחים

גדולים (BIG DATA) \ Data Lake. ניהול ותחקור המידע – כלי תחקור, מנועים ועיבוד נתונים: BI, (Business Intelligent, Data DM, LA, ML, LLM Mining, Link Analysis, Machine Learning, Large Language Model) או כל יכולת אחרת רלוונטית ואופן השמירה על אבטחת ומשילות המידע.

2.1.2.1.17.3. הצגת האירועים/הג"מים ע"ג מפות אינטראקטיביות.

2.1.2.1.17.4. סימולציה לביצוע אנליזות לתמיכה בתהליכי ניהול אירוע.

2.1.2.1.18. יש לפרט את כלל הממשקים במערכת, יכולות פונקציונאליות במערכת, הכלים, הנהלים ותהליכים שמתבצעים בזמן אירוע, ניהול הרשאות והזדהויות, גישה ממודרת לתכנים, ניהול אירועים, אפליקציות, תוכנות עזר, מוצרי מדף, כלי תחקור וניתוח לאחור.

2.1.2.1.19. יש לפרט את השלבים ואת כל תהליך ה- WORK FLOW בניהול של אירוע סייבר מתגלגל: איסוף, איתור, מחקר ואנליזה, ניהול אירועים ויצירת תמונת מצב, הכלה, תגובה ומניעה. (יש לספק דוגמא עבור תהליך ה- WORK FLOW).

2.1.2.1.20. יש לפרט את ארכיטקטורת רשת התקשורת שבין הג"מים למרכז ה TSOC בתצורת HUB AND SPOKE- סוג ציוד התקשורת ואופן ניהולו במרכז ה TSOC, רוחב הפס שישמש לקישור אתרים מרוחקים, הצפנת תעבורה, ניטור החיבור, בדיקת תאימות למוצרי האבטחה ועדכוני אבטחה, נרמול ופילטר מאפיינים מזהים ועמידה בתנאי ה SLA –ע"פ דרישות המכרז. יש להרחיב על אופן צמצום התעבורה בצד לקוח, על ידי הפתרון המוצע, באופן כזה שיאפשר מידע ערכי ככל האפשר לניתוח במערכת הSIEM- ומצד שני אגירת מידע משמעותי ככל האפשר בצד לקוח כך שבעת אירוע תוכל התשתית להוות כלי חקירתי.

2.1.2.1.21. יש לפרט את ארכיטקטורת כלל המערכות בתצורת הענן כולל מרכיבי תשתיות האבטחה למרכז ה TSOC, רשת התקשורת, החומרה, רכיבי ההגנה כגון FW, כלי

הגנת וניטור הענן והאינטגרציה למערכות השונות מתצורת SaaS או IaaS.

2.1.2.1.22. יש לבצע תכנון הגירת הג"מים כיום והחוקים הקיימים בשימוש ה-SOC הנוכחי ולשלב בתהליך ההקמה.

2.1.2.1.23. המזמין שומר לעצמו את הזכות הבלעדית להורות לספק על הגירת פעילות ה TSOC-לתשתיות פרויקט 'כיפת הסייבר' של מערך הסייבר הלאומי מבוסס (Chronicle), כולן או חלקן.
למימוש זכות זו, על הספק להגיש לאישור המשרד, כחלק מתוצרי שלב ההקמה, תוכנית הגירה עקרונית המפרטת את המשמעויות הטכנולוגיות והתפעוליות של המעבר.
המעבר לתשתיות אלו יבוצע על פי דרישת המשרד בכתב, ובכלל זה עם מימוש האופציה להארכת ההתקשרות (כ-24 חודשים ממועד חתימת ההסכם) או בכל מועד אחר שיקבע המזמין החל ממועד זה.
הספק מתחייב כי הארכיטקטורה והכלים שיוצעו על ידו במועד הגשת ההצעה יאפשרו תאימות טכנולוגית (Interoperability) למערכת Chronicle באופן שיבטיח הגירה חלקה ללא אובדן מידע או פגיעה ברציפות התפקודית של המרכז.

2.1.2.1.24. אפיון מפורט עבור מערכת ניהול TSOC ואירועי סייבר. מערכת שו"ב לניהול אירוע סייבר ב- TSOC תאפשר תגובה יעילה, מהירה ומדויקת לניהול, תיעוד, ניתוח, יכולת אחזור אירועי עבר, והפקת דוחות התומכת בפעילות בזמן שגרה ובזמן חרום .

2.1.2.1.25. יש לפרט את המדיניות, הנהלים והתהליכים לגבי אופן ההפעלה והתפקוד במהלך אירועים מסוגים שונים.

2.1.2.1.26. מערכת השו"ב המרכזית – (תאפשר ניהול הטיפול באירועי סייבר, תיעוד האירועים, ניהול תהליך הטיפול באירוע שלב אחר שלב, יכולת אחזור אירועי עבר קשורים

(קורלציות) , הפקת דוחות, יצוא דוחות, תיעוד פעולות, ניהול משמרות, כלי ניהול ומודל תומך החלטה.

2.1.2.1.27. משך אגירת המידע במערכת המוצעות בפתרון יהיה לכל הפחות לשנתיים.

2.1.2.1.28. יש לוודא כי כלל המערכות והתוכנות ימצאו לאורך כל תקופת ההתקשרות ברישוי ותחזוקה מלאה מצד היצרנים. (ללא שימוש במערכות בשלב EOS/EOL). במידה ובמהלך ההתקשרות אחד המוצרים/מערכות יוגדר ע"י היצרן כ EOL/EOS- באחריות המציע לספק חלופה על חשבונו טרם ההגעה ל EOL/EOS.

2.1.2.1.29. איסוף המידע, ניתוח ואיתור המידע יתבצע בהתאם לפורמטים ולדרישות בהתאם למקורות עיקריים הבאים:

2.1.2.1.29.1. מידע מהג"מים – כ-50 ג"מים - המידע ייאסף הן ע"י ממשק אוטומטי והן באופן ידני או חצי ידני (הכנסת קבצי מידע רלוונטיים).

- חיבור לתשתיות ניטור בג"מים על בסיס הפתרון הטכנולוגי המוצע על ידי הספק על ידי התקנת כלי איסוף לאירועי האבטחה בג"מים על ידי הזוכה תוך תכנון מוקפד ליצירת תנאים מינימליים לשינוי או השפעה בגוף המנוטר.

2.1.2.1.29.2. חיבור לתשתיות סנסורים (שכבה נוספת) בג"מים על בסיס הפתרון טכנולוגי המוצע על ידי הספק על ידי התקנת כלי איסוף ייעודי בג"מים על ידי הזוכה (על פי דרישת המשרד).

2.1.2.1.29.3. מידע מודיעין מסחרי ממקורות חיצוניים ואחרים ייאסף באמצעות ממשק אוטומטי.

2.1.2.1.29.4. הזנת אירועים ממקורות מידע חיצוניים נוספים רלוונטיים באופן אוטומטי לדוגמא MISP.

2.1.2.1.30. בפתרון יש לפרט ארכיטקטורה מקיפה של הפתרון והשירותים כנדרש בסעיפים 2.1.2.2 – 2.1.2.4, מוצרים, איוש הצוות והמערכות.

2.1.2.2. **מערכת "על" - SIEM OF SIEM'S (S) - הרחבה בסעיף 2.1.3**

ה- SIEM נדרש להיות מקטגוריית SIEM המובילות על בסיס מדד Gartner (באחד מ-3 הדו"חות האחרונים) ללא מוצרים נישתיים (Niche players) המהווה מערכת מרכזית לקורלציות אירועים והצגתם כחלק מתמונת המצב המגזרית:

א. ביצוע קורלציות של חומרים הנאספים מהארגונים המבוזרים במגזר, דרך תקשורת מאובטחת נפרדת מזו של הארגון.

ב. הצגת תמונות ה-SIEM'S בג"מים לכדי תמונה אחת כוללת ומוכלת במרכז ה-TSOC בזמן אמת או קרוב לזמן אמת.

ג. ניתוחים, הפקת דוחות ואיתור של פעילויות חשודות משותפות בחתך רוחבי של המגזר, חוצה-ארגון (שונה מהראייה של הארגון הבודד).

ד. המערכת תאפשר שיקוף התמונה לג"מים באופן כזה שיוכלו לראות את נתוניהם בלבד.

ה. אפיון מדויק ופרטני לדרישות מערכת "על" יבוצע בתאום מלא עם המשרד בשלב התכנון המפורט של הפרויקט.

2.1.2.3. **פתרון שו"ב מרכזית (S) הרחבה בסעיף 2.1.4**

הפתרון יהווה את מרכז השליטה והבקרה (שו"ב) הראשי של מרכז ניהול האבטחה TSOC ויאפשר את ניהול המרכז, ניהול הטיפול באירועי סייבר, יתממשק למערכת SIEM המרכזית, יתעד את האירועים, יקיים יכולת חיפוש ואחזור אירועי עבר קשורים (קורלציות), הפקת דוחות, יצוא דוחות, תיעוד פעולות, ניהול משמרות, ניהול פרטי אנשי קשר לקוחות בג"מים, כלי ניהול ומודל תומך החלטה. הפתרון יכיל מערכות ויקיים קשרים ופונקציונליות מלאה שתשקף תהליכים שלמים בתפיסת ההפעלה של מערכת ה TSOC תוך קיום Interoperability בין מערכות (כלל המערכות או כל אחת לחוד תהינה מקטגוריית המובילות על בסיס מדד Gartner (באחד מ-3 הדו"חות האחרונים) ללא מוצרים נישתיים (Niche players):

א. מערכת ניהול לקוחות בסגנון מערכת - CRM

ב. מערכת ניהול קריאות בסגנון מערכת - TICKETING

ג. מערכת ניהול תהליכי עבודה ואישורים בסגנון מערכות - WORKFLOW

ד. מערכת שיתוף מידע מאובטח בסגנון מערכות MANAGED FILE TRANSFER.

ה. מערכת מאגר הסייבר המרכזי ומערכת מחקר, ניתוח והעשרת מידע -תשתית מידע אחודה, מבוססת טכנולוגיית BIG DATA \ DATA LAKE המאפשרת לאגור את כלל המידע לטווח קצר ולטווח ארוך. המודול יאפשר לבצע מחקר וניתוח של אירועי סייבר מעל תשתית מאגר הסייבר המרכזי ומשתמשת ככלי ניהול, ניתוח והעשרת המידע.

ו. מערכת תזמור (Orchestration), אוטומציה (Automation) ותגובה (Response) בסגנון מערכות SOAR

ז. מערכת השו"ב תאפשר מענה חוצה ארגונים כך שמענה לאירוע שנפתח ע"י המרכז יוכל לקבל מענה בגוף מונחה ולהיבחן/להיסגר ע"י המרכז.

2.1.5 הרחבה בסעיף (S) TSOC <u>תשתיות אבטחה למרכז</u> .2.1.2.4

מערכות אבטחה היקפיות המספקות את חוסן המענה לאבטחת מרכז ה) TSOC כולם מקטגוריית המובילות על בסיס מדד Gartner (באחד מ-3 הדו"חות האחרונים) ללא מוצרים נישתיים (Niche players) התשתיות יכללו מערכת מהקטגוריות הבאות :

הגנת רשת	מערכת חומת אש Firewall ברמת מיקרו-סגמנטציה
	מערכת חומת אש אפליקטיבית Web Application Firewall (WAF)
	מערכת אבטחת ממשקים (API Gateway)
	מערכת DDoS Protection
	מערכת גישה מאובטחת מרחוק SSE
אבטחת מידע	מערכת לזיהוי הימצאות מידע רגיש (DSPM ו-DLP)
	מערכת להעברת קבצים מנוהלת (MFT)
	ניהול מכשירים ניידים (MDM) ואפליקציות (MAM)
פוגענים ונוזקות	מערכת זיהוי ושיקום ברמת מערכות הפעלה, עמדות הקצה וקונטיינרים (Container Runtime, XDR וכד')
	מערכת הלבנת קבצים (CDR + Sandbox)
	ארגז חול פוגענים (Sandbox)
הגנת סביבת ענן	כל המידע והשרתים במערכת צריכים להיות מוצפנים באמצעות מערכת ההצפנה המובנת של ספק הענן (CSP) כאשר ניהול המפתחות בשליטת המציע (CMK).
	פלטפורמה להגנת סביבת הענן ותצורת האבטחה כגון (CNAPP, CASB, CloudDR,SSE)
	מערכת ניהול מפתחות וסודות (KMS)
ניטור ותגובה	מערכת ניהול התראות אבטחה מרכזית (SIEM) – (אחודה עם מערכת "על" - SIEM OF SIEM'S)
	מערכת גילוי משטחת תקיפה חיצוני (VAS\EASM)
	מערכת איסוף מודיעין מסחרי (Threat Intelligence)
	מערכת תגובה לאירועים באופן אוטומטי (SOAR) – אחודה עם המערכות התומכות של המרכז)
ניהול זהויות	מערכת ניהול זהויות מרכזית וניטור הרשאות ענן (IDP+IAM+CIEM מרכזי שיאפשר שליטה על כל הזהויות)

2.1.3. **<u>מערכת "על" - SIEM OF SIEM'S</u> לאיסוף והצגה של אירועי אבטחה ממערכות SIEM (Security Information & Event Management) בג"מים (M)**

תפקידה של מערכת לקבל, לנתח לתייג ולהציג אירועי אבטחת מידע ממערכות אבטחה בג"מים וממערכות ה SIEM אשר נמצאים בג"מים השונים. תפקיד "על" של המערכת הינו ביצוע קורלציות של חומרים הנאספים מג"מים במגזר, ניתוחים והפקת דוחות ואיתור של פעילויות חשודות משותפות בחתך רוחבי של המגזר, חוצה-מגזר, תוך ייצור של שכבת אנליזה ואיתור נוספת בראיית המגזר (שונה מהראייה של הארגון הבודד.

1.1. הערכת נפחים – עד 50 ג"מים בגודל שונה.

1.2. ג"מ קטן – עד 2000 .EPS עד 10 גופים.

1.3. ג"מ בינוני - 2000-5000 EPS. כ-25 גופים.

1.4. ג"מ גדול – מעל 5000 EPS. עד 15 גופים.

1.5. **<u>דרישות יכולות איסוף</u>** - על המציע לפרט את עמידתו בדרישות הבאות:

1.6. יכולת קבלת מידע מרכיבים מנוטרים (המציע יפרט את מוצרי התשתית העיקריים אותם המערכת יודעת לנטר OUT OF THE BOX כמו גם מערכות הפעלה עיקריות

2.1.3.1.1. יכולת עיבוד - המציע יפרט מהם אלגוריתמי העיבוד של המערכת, יתרונות המערכת בהיבט ניהול זמני העיבוד לאור האלגוריתמים בשימוש.

2.1.3.1.2. פירוט על יכולת איסוף על ידי כלי ייעודי שיוגדר בצד הג"מ על ידי המציע.

2.1.3.1.3. יכולות הקורלציה של אירועים בין רכיבים שונים, מוצרי תשתית שונים ובעיקר בין הארגונים השונים במגזר (תצורת SIEM OF SIEM'S בכולל ניטור סביבות ענן, ON PREM, פלטפורמות תחבורתיות מסוגים שונים, סביבות תפעוליות וסביבות IOT שונות.

2.1.3.1.4. התממשקות למערכות MISP בממשק NATIVE.

2.1.3.1.5. יכולת התממשקות למערכות SIEM ומוצרי אבטחה נוספים הקיימים בג"מים במגזר ו/או התקנת רכיב איסוף שמסוגל לבצע את הפעולות הבאות:

- איסוף המידע בצד הג"מ - סינון, פילטור ודחיסה של המידע.
- אגריגציה של המידע ושידור לתשתית מרכז אבטחת הסייבר TSOC.
- תיקון זמנים במרכז (לדוגמה: GMT מול שעון ישראל GMT-2H)
- תיוג האירוע – מתן תג אירוע אחד עבור הקורלציות בכל המגזר.
- תיוג של תחנה או התקן פנימי ע"י: NAME RESOLUTION + IP.

2.1.3.1.6. יכולות אגריגציה של מספר אירועים לכדי אירוע יחיד.

2.1.3.1.7. יכולת שליטה ובקרה בקצב העברת המידע ובקרה על העמסת רוחב הפס של הארגון.

2.1.3.1.8. המציע יפרט לגבי יכולות איסוף של המידע ועמידה בתקנים הסטנדרטים אשר מתקבלים ממערכות ה- SIEM המותקנים בג"מים השונים.

2.1.3.1.9. המציע יפרט את דרך איסוף האירועים של המערכת מכל אחד מהרכיבים.

2.1.3.1.10. המציע יפרט לגבי יכולות המערכת בעבודה עם AGENT ו/או AGENT-LESS.

2.1.3.1.11. על המציע לפרט את תהליך איסוף האירועים המנורמלים ממערכות ה- SIEM ומערכות האבטחה הנוספות בג"מים השונים.

1.7. תמיכה באיסוף מידע באמצעות הפרוטוקולים והסטנדרטים הבאים:

- SECURE API
- SYSLOG
- SNMP V3
- FTP/S-FTP/FTP-S
- WEB SERVICE
- WMI
- CEF
- CSV FILES PROCESS CAPABILITY
- TXT FILES PROCESS CAPABILITY

2.1.3.1.12. יכולת נרמול של לוגים בתצורות שונות ללוגים ידועים בפורמט שהמערכת מכירה.

2.1.3.1.13. יכולת ניתוח של לוגים טקסטואליים.

2.1.3.1.14. יכולת איסוף בתשתית מבוזרת (NON-DOMAIN).

המציע מוזמן לספק כל מידע נוסף רלוונטי מטעמו בנושא זה. המשרד אינו מתחייב לקבל מידע זה ו/או לפעול על פיו.

2.1.3.2. **<u>דרישות קורלציה ואגרגציה</u>** – על המציע לפרט את עמידת המערכת בדרישות הבאות:

2.1.3.2.1. יכולת להגדרת קורלציה המעידות על התרחשות אירוע החוצה מספר רחב של מערכות ו/או חוצי ארגונים, הבדלה בין מערכות תשתיתיות לבין מערכות אפליקטיביות.

2.1.3.2.2. יכולת קורלציה בין כתובות חיצוניות (בעולם) לכתובות פנימיות.

2.1.3.2.3. יכולות אגריגציה של לוגים המעידים על אותו האירוע.

המציע מוזמן לספק כל מידע נוסף רלוונטי מטעמו בנושא זה. המשרד אינו מתחייב לקבל מידע זה ו/או לפעול על פיו.

2.1.3.3. **<u>דרישות חקר אירועים</u>** - על המציע לפרט את עמידת המערכת בדרישות הבאות:

2.1.3.3.1. על המציע לפרט מהו מנגנון האחסון לאירועים לטווח ארוך (שמירה של אירועים בטווח שמעל לשנה) וטווח קצר [LIVE INFORMATION] (עד לשנה), אשר יאפשר שליפת נתונים מהירה במידה ויידרש תחקור לאחור.

2.1.3.3.2. על המציע לפרט מהו מנגנון ארכוב אירועים תוך שליפה בזמן קצר של טווחי נתונים משתנים ועל פי חיתוכים והתניות שונות- דוגמא: סך האירועים, בתאריך מסוים, ל-IP מסוים, לאירוע מסוים/ למעט אירוע מסוים.

2.1.3.3.3. המערכת תאפשר דחיסת נתונים, שנשמרים לזמן ממושך. על המציע לפרט מהם יחסי הדחיסה.

2.1.3.3.4. המערכת תאפשר יכולת מחיקת נתונים היסטוריים לפי תאריך ו/או כל פרמטר אחר. המציע יפרט במידה וקיימים פרמטרים נוספים למחיקה.

2.1.3.3.5. המערכת תאפשר יצוא נתונים למערכת חיצונית באמצעות ממשק אוטומטי או חצי אוטומטי או ידני.

2.1.3.3.6. על המציע לפרט מהי שיטת אגירת האירועים בבסיס נתונים/ בשרת הנתונים.

2.1.3.3.7. יכולת ניטור ובקרה מקיפים (לא כאירועים בודדים אלא כמכלול) ברשת כולה. לדוגמא- אירוע שהחל ב PERIMETER ומתפשט לשירותים שונים ברשת יוצג כאירוע אחד שאותו ניתן יהיה לחקור ולפרק לאירועים בודדים.

2.1.3.3.8. יכולת ביצוע שאילתות מבוזרות על נפחי מידע גדולים.

המציע מוזמן לספק כל מידע נוסף רלוונטי מטעמו בנושא זה. המשרד אינו מתחייב לקבל מידע זה ו/או לפעול על פיו.

2.1.3.4. **<u>דרישות ניהול אירוע</u>** - על המציע לפרט את עמידתו בדרישות הבאות:

2.1.3.4.1. ניהול אירוע (CASE MANAGEMENT) - רישום סטאטוס אירוע, מעקב אחר טיפול באירוע, דרכי ההחלטה של המערכת על הפנייה של אירוע, סוגי אירועים במערכת וכו'.

2.1.3.4.2. יכולות איתור בדיעבד של אירועים על ידי מנגנון חיפוש מובנה במערכת, על המציע לתאר בצורה מפורטת איך בנוי מנגנון החיפוש, שדות החיפוש, פונקציות חיפוש וכד'.

2.1.3.4.3. יכולות אסקלציה של אירועים, קביעת ספים בגינם אירועים יועברו לידיעת רמה ממונה.

2.1.3.4.4. יכולת העברת משימות, האצלת סמכויות וניהול מבוזר של משימות ע"י המערכת.

2.1.3.4.5. יכולת התממשקות לרכיבי רשת וביצוע פעולות אקטיביות.

המציע מוזמן לספק כל מידע נוסף רלוונטי מטעמו בנושא זה. המשרד אינו מתחייב לקבל מידע זה ו/או לפעול על פיו.

2.1.3.5. **<u>דרישות ניהול חוקים</u>**- על המציע לפרט את עמידתו בדרישות הבאות, באופן המפורט להלן:

1.8. על המציע לפרט עד 30 חוקים מובנים במערכת (OUT OF THE BOX)מהם המשרד יוכל להתרשם.

2.1.3.5.1. יכולת כתיבת חוקים ע"ב כלי עזר כדוגמת DRAG AND DROP של אובייקטים, שימוש בשפות קוד, שימוש באשפים מובנים במערכת.

2.1.3.5.2. יכולת כתיבת חוקים ע"ב שאילתות מול בסיס הנתונים.

2.1.3.5.3. יכולת בחינת חוקיות ויעילות החוקים- באילו דרכים ניתן לבדוק במערכת את האפקטיביות של חוקים שנכתבו באילו דרכים במערכת ניתן לבדוק את החיות של החוקים

2.1.3.5.4. יכולת קביעת חומרה (SEVERITY) וביצוע אגריגציה של חומרת האירועים לאירוע מרכזי אחד.

2.1.3.5.5. יכולת ייבוא חוקים מארגונים אחרים המשתמשים באותה מערכת.

2.1.3.5.6. בנוסף יעביר המשרד כ-10 תרחישים אשר המציע יידרש להראות כיצד הוא נותן להם מענה כיום/נערך לתת להם מענה במסגרת ה POC.

2.1.3.5.7. סט רחב של חוקים גנריים- על המציע לפרט כמה חוקים בסה"כ מובנים במערכת (OUT OF THE BOX).

2.1.3.5.8. יכולת לבצע השתקה לחוקים פר ג"מ, שתקה בכמה רמות: ביטול ההתרעה לגמרי ,התרעה ברמת אינדיקציה שנשארת פנימית אצלנו לשם תחקור בעת אירוע בהמשך ,התרעה במייל מלבד, התרעה מהותית.

המציע מוזמן לספק כל מידע נוסף רלוונטי מטעמו בנושא זה. המשרד אינו מתחייב לקבל מידע זה ו/או לפעול על פיו.

2.1.3.6. **<u>סנכרון שעונים וניהול זמנים</u>** - על המציע לפרט את עמידתו בדרישות הבאות:

2.1.3.6.1. פורמט השדות המתארים תאריך ושעה יהיה זהה בכל האירועים המנוהלים במערכת.

2.1.3.6.2. פורמט הזמן יהיה זהה הן בשמירת הנתונים בבסיס הנתונים והן בהצגתם.

1.9. המערכת תבצע סנכרון זמנים בהתאם לשעון של המרכז על מנת שניתן יהיה לזהות אירועים, שהתרחשו באותו הזמן, גם אם השעונים במקורות המידע המדווחים עליהם מכוונים לשעה שונה .

2.1.3.6.3. ביצוע סנכרון זמנים לא יפגע בערך שדה ה-"תאריך/שעה" באירוע המקורי. יש לתאר כיצד מבוצע סנכרון הזמן במערכת.

המציע מוזמן לספק כל מידע נוסף רלוונטי מטעמו בנושא זה. המשרד אינו מתחייב לקבל מידע זה ו/או לפעול על פיו.

2.1.3.7. **<u>דרכי התראה על אירוע וביצוע פעולות בעקבות אירוע</u>**

- על המציע לפרט את עמידתו בדרישות הבאות:

2.1.3.7.1. יכולות חיווי מובנות במערכת- צלילים, מסכים קופצים, שימוש בצבעים, יכולות גרפיות כגון שדות מודולריים, יכולות לשתול במערכת טקסט קבוע אותו המשרד מבקש להכניס בהתרחש אירוע.

2.1.3.7.2. יכולות פתיחת אירוע (CASE) כחלק מניהול האירועים (CASE MANAGEMENT) יכולת שליחת הודעות דרך מערכות דואר אלקטרוני, SMS, התראות וכד' במוצר עצמו ובינו לבין מערכת השו"ב שתוקם על ידי הזוכה.

2.1.3.7.3. יכולת ביצוע פעולות כתגובה להתרחשות אירוע. פעולות הכוללות הפעלת תוכניות ומערכות חיצוניות.

2.1.3.7.4. יכולות סגירת אירוע - אישור רמה ממונה תוך שילוב מערכת ניהול תהליך במערכת השוב שתוקם על ידי הזוכה.

המציע מוזמן לספק כל מידע נוסף רלוונטי מטעמו בנושא זה. המשרד אינו מתחייב לקבל מידע זה ו/או לפעול על פיו.

2.1.3.8. **<u>ממשק משתמש</u>** - על המציע לפרט את עמידתו בדרישות הבאות:

2.1.3.8.1. גמישות בהצגת הנתונים - המערכת תאפשר גמישות מרבית בהצגת נתונים. לצורך כך תכיל המערכת ממשק משתמש שיאפשר למיין את הנתונים לפי שדות שונים.

2.1.3.8.2. המערכת תאפשר את הצגת הנתונים בצורה גראפית מלאה, בתצוגה של מפות רשת ומפות גיאוגרפיות בתצורות שונות, ועם נתונים לפי דרישות המשתמשים ברמות הניהול השונות (יינתן יתרון לתמיכה בעברית).

2.1.3.8.3. המערכת תכלול ממשק משתמש נוח וקל, שיאפשר למשתמשים ברמות השונות לבנות ולהתאים לעצמם תצוגות אישיות לצורך תצוגה והבנה נכונה ומהירה של המצב.

2.1.3.8.4. המערכת תכלול ממשק משתמש מרכזי וידידותי, שיאפשר למנהלי המערכת צפייה, חקירה, טיפול בדוחות, מתן הרשאות כתיבה ושינוי חוקים. על המציע לצרף צילומי מסך של הממשק המרכזי.

2.1.3.8.5. על המערכת להיות בעלת ממשק היררכי כך שהמעבר בין אובייקטים במסך יהיה בסדר היררכי

2.1.3.8.6. המציע יתאר שימוש המערכת בגרפים ותרשימים אינטואיטיביים למשתמש.

2.1.3.8.7. המציע יתאר יכולת חקירה מלאה וקבלת נתונים מתוך מסך התחקור על האובייקטים המעורבים באירוע.

2.1.3.8.8. המציע יתאר שימוש בפקדים שונים.

2.1.3.8.9. על המערכת להיות בעלת יכולת קבלת נתונים מקיפה על כל אובייקט במסך התחקור של אירוע (IP ADDRESS, MAC ADDRESS, SEGMENT, DNS NAME וכד')

2.1.3.8.10. שימוש בטבלאות נתונים במסך התחקור.

2.1.3.8.11. יכולות התאמה של המסך לרצון המשתמש- הגדלה/ הקטנה של תתי חלונות, הבלטה של אובייקטים, שימוש בצבעים.

2.1.3.8.12. יכולת DRAG AND DROP של אובייקטים לתחקיר ו/או לצורך הפקה של דוחות.

המציע מוזמן לספק כל מידע נוסף רלוונטי מטעמו בנושא זה. המשרד אינו מתחייב לקבל מידע זה ו/או לפעול על פיו.

2.1.4. **<u>פתרון שו"ב מרכזי</u> (M)**

הפתרון יהווה את מרכז השליטה והבקרה (שו"ב) הראשי של מרכז ניהול האבטחה TSOC ויאפשר את ניהול המרכז, ניהול הטיפול באירועי סייבר, יתממשק למערכת SIEM המרכזית, יתעד את האירועים, יקיים יכולת חיפוש ואחזור אירועי עבר קשורים (קורלציות) , הפקת דוחות, יצוא דוחות, תיעוד פעולות, ניהול משמרות, ניהול פרטי אנשי קשר לקוחות בג"מים, כלי ניהול

ומודל תומך החלטה. הפתרון יכיל מערכות ויקיים קשרים ופונקציונליות מלאה שתשקף תהליכים מתפיסת ההפעלה של מערכת ה TSOC תוך קיום Interoperability בין מערכות. הספק יכול לבחור לאחד בין מערכות ובתנאי שמקיימות הדרישות והפונקציונליות המלאה של כלל יכולות (כלל המערכות או כל

אחת לחוד תהינה מקטגוריית המובילים על בסיס מדד Gartner (באחד מ-3 הדו"חות האחרונים):

2.1.4.1. **<u>מערכת ניהול לקוחות בסגנון מערכת – CRM</u>**

2.1.4.1.1. המערכת תשמש לניהול לקוחות, ספקים ושירותים הקשורים למרכז TSOC.

2.1.4.1.2. המערכת תאפשר מעקב וניהול אירועי אבטחה מול לקוחות המרכז.

2.1.4.1.3. המערכת תאפשר אינטגרציה עם SIEM, SOAR ומערכות אבטחה אחרות לקבלת מידע על אירועים ותקריות בזמן אמת.

2.1.4.1.4. המערכת תתמוך בניהול משימות בהתאם ל-SLA ותייצר דוחות עבור צוות TSOC המשקף מצב טיפול באירועים פתוחים וסטטיסטיקות עבר.

2.1.4.1.5. המערכת תספק ממשק אינטואיטיבי ודינמי עם תמיכה בעברית ובאנגלית.

2.1.4.2. **<u>מערכת ניהול קריאות בסגנון מערכת - TICKETING</u>**

2.1.4.2.1. המערכת תשמש לניהול קריאות שירות ומעקב אחר אירועי סייבר שנוצרות על ידי צוות ה-TSOC, מול לקוחות המרכז וספקים.

2.1.4.2.2. המערכת תאפשר מעקב אחר סטטוס אירועי האבטחה, תיעוד פעולות, והקצאת משימות לצוותים ולגורמים רלוונטיים.

2.1.4.2.3. המערכת תאפשר אינטגרציה מלאה עם SIEM, SOAR ומערכות אבטחה נוספות לקבלת מידע על אירועים אוטומטית.

2.1.4.2.4. המערכת תתמוך בניהול SLA (SERVICE LEVEL AGREEMENT) ותבטיח מעקב דינאמי אחר טיפול בקריאות בהתאם לזמני התגובה והטיפול הנדרשים.

2.1.4.2.5. המערכת תספק ממשק משתמש אינטואיטיבי ודינמי, עם תמיכה בעברית ובאנגלית.

2.1.4.2.6. המערכת תתממשק למערכות דיווח באמצעות דוא"ל וממשקי API אל מול מערכות כגון WhatsApp ו Telegram.

2.1.4.3. **<u>מערכת ניהול תהליכי עבודה ואישורים בסגנון מערכות - Workflow</u>**

2.1.4.3.1. המערכת תשמש לניהול תהליכי עבודה אוטומטיים ותזמור משימות (Orchestration) בין צוותי TSOC, מערכות אבטחת מידע ולקוחות.

2.1.4.3.2. המערכת תאפשר יצירה, ניהול ומעקב אחרי Workflows מותאמים אישית לניהול אירועי אבטחה, תגובה לאירועים וחקירות אבטחה – בין היתר יתאפשר תהליך בניית תהליך באמצעות מעצב Designer Drag&Drop.

2.1.4.3.3. המערכת תתמוך באינטגרציה מלאה עם SIEM, SOAR, EDR, מערכות ניהול קריאות (Ticketing), ITSM ומערכות דוחות.

2.1.4.3.4. המערכת תאפשר שיתוף פעולה בין צוותים על בסיס זרימות עבודה מתוזמרות ואוטומטיות.

2.1.4.3.5. המערכת תספק תצוגת לוח מחוונים (Dashboard) בזמן אמת להצגת מצב התהליכים הפעילים, הביצועים סטטיסטיקות.

2.1.4.3.6. **<u>מערכת שיתוף מידע מאובטח בסגנון מערכות Managed File Transfer.</u>**

2.1.4.3.6.1. המערכת תאפשר העברה מאובטחת של קבצים בין צוותי TSOC, גורמים פנימיים בין המרכז למשרד, שותפים עסקיים, הג"מים ולקוחות חיצוניים.

2.1.4.3.6.2. המערכת תספק ניהול מבוקר ומעקב מלא אחר קבצים שהועברו, כולל בקרת גישה, לוגים ויכולת שחזור.

2.1.4.3.6.3. המערכת תאפשר ניהול הרשאות מבוסס תפקידים (RBAC - Role-Based Access Control) לקבוצות משתמשים וצוותים שונים – מבלי לגרוע מהאמור המערכת תאפשר שיתוף של קבצים באופן מבוקר למשתמשים חיצוניים ללא הזדהות "Guest".

2.1.4.3.6.4. המערכת תאפשר יכולת "צפיה חד פעמית" במידע.

2.1.4.3.6.5. המערכת תאפשר שליטה מלאה ביכולת ההורדה, הצפייה, העריכה והעדכון של המידע המשותף.

2.1.4.3.6.6. המערכת תאפשר שילוב עם פתרונות Data Loss Prevention (DLP) לזיהוי ומניעת דלף נתונים רגישים.

2.1.4.3.6.7. המערכת תספק יכולת סריקה לאיתור קבצים חשודים או נגועים (Antivirus & Sandboxing Integration).

2.1.4.3.7. **<u>מערכת מאגר הסייבר המרכזי ומערכת מחקר, ניתוח והעשרת מידע -תשתית מידע אחודה, מבוססת טכנולוגיית BIG DATA \ DATA LAKE</u>**

2.1.4.3.7.1. המערכת תאפשר לאגור את כלל המידע לטווח קצר ולטווח ארוך.

2.1.4.3.7.2. המערכת תאפשר לבצע מחקר וניתוח של אירועי סייבר מעל תשתית מאגר הסייבר המרכזי ומשתמשת ככלי ניהול, ניתוח והעשרת המידע.

2.1.4.3.7.3. המערכת תשמש כמאגר מרכזי לאיסוף ואיחוד נתונים ממקורות שונים, כולל SIEM, SOAR, EDR, DLP, מערכות ניהול זהויות (IAM) ומודיעין איומים (Threat Intelligence).

2.1.4.3.7.4. המערכת תאפשר אחסון מבוזר וסקלאבילי לניהול כמויות נתונים גדולות, עם תמיכה בעיבוד בזמן אמת (Streaming) ועיבוד נתונים היסטוריים (Batch).

2.1.4.3.7.5. המערכת תתמוך במודל DATA LAKE המאחסן נתונים גולמיים בפורמטים שונים (STRUCTURED, SEMI-STRUCTURED, UNSTRUCTURED).

2.1.4.3.7.6. המערכת תספק יכולת ניתוח מתקדם, כולל מנועי חיפוש ואינדוקס, חקירת אירועים מבוססת ML,AI וניתוח אנומליות (מבלי לחשוף או לשתף את המידע עם הגורם צד ג' או יכולות עיבוד חיצוניות למערכת).

2.1.4.3.7.7. המערכת תתמוך באינטגרציה עם כלי BIG DATA ו-ML, כגון APACHE SPARK, KAFKA, HADOOP, TENSORFLOW ו-ELK STACK.

2.1.4.4. **<u>מערכת תזמור (ORCHESTRATION) , אוטומציה (AUTOMATION) ותגובה (RESPONSE) בסגנון מערכות SOAR</u>**

2.1.4.4.1. **דרישות כלליות:**

2.1.4.4.1.1. המערכת תשמש לניהול תקריות אבטחת מידע (INCIDENT RESPONSE) באופן אוטומטי ומבוסס תהליכים (PLAYBOOKS & WORKFLOWS).

2.1.4.4.1.2. המערכת תספק תזמור (ORCHESTRATION) מלא בין כלי אבטחת מידע שונים הקיימים בפתרון המוצע על ידי הספק.

2.1.4.4.1.3. המערכת תאפשר אינטגרציה דו-כיוונית עם SIEM, פתרונות EDR/XDR, מערכות FIREWALL, מערכות ניהול זהויות (IAM), פתרונות מודיעין איומים (TIP), מערכות דואר אלקטרוני ועוד.

2.1.4.4.1.4. המערכת תאפשר התאמה אישית של תהליכי תגובה בהתאם לצרכי הארגון ובהם יכולות כגון: העשרת אירועים ממקורות שונים, השלמת פעולות אוטומטיות וחצי אוטומטיות, השלמת פעולות חקירה תוך הפעלת כלים נוספים.

2.1.4.4.1.5. המערכת תכלול ממשק ניהול מרכזי, קל לשימוש ועם יכולות DASHBOARD לניטור בזמן אמת.

2.1.4.4.2. **<u>דרישות פונקציונליות:</u>**

2.1.4.4.2.1. **<u>ניהול ואוטומציה של תגובות לאירועים:</u>**

א. המערכת תתמוך בבניית PLAYBOOKS אוטומטיים לניהול ותגובה לאירועים, עם יכולת התאמה אישית.

ב. המערכת תאפשר הפעלת תהליכי תגובה אוטומטיים, כולל ניתוח נתונים, שליפת מידע מגורמי צד ג' וביצוע פעולות מתקנות.

ג. המערכת תאפשר תגובה בזמן אמת לתקריות על בסיס חוקים מוגדרים מראש.

ד. המערכת תכלול מנגנון אישור אנושי (HUMAN-IN-THE-LOOP), שבו ניתן להגדיר שלבים שדורשים אישור ידני.

2.1.4.4.2.2. **<u>ניתוח ואינטגרציה עם מערכות קיימות:</u>**

א. המערכת תתמוך באינטגרציה עם פתרונות SIEM, EDR/XDR, IDS/IPS, DLP, AV, NAC, FW ועוד.

ב. המערכת תאפשר שליפה ואנליזה של מידע ממערכות מודיעין איומים (THREAT INTELLIGENCE PLATFORMS - TIP).

ג. המערכת תאפשר אוטומציה של חקירת אירועים, כולל חיפוש אוטומטי בנתוני לוגים וקורלציה עם מקורות מידע נוספים.

2.1.4.4.2.3. **<u>תיעוד, מעקב ותחקור תקריות:</u>**

א. המערכת תכלול מנגנון תיעוד לכל תקרית, כולל תיעוד מלא של כלל הפעולות שבוצעו.

ב. המערכת תתמוך ביכולת מעקב אחר סטטוס טיפול בתקריות ולוחות זמנים מוגדרים (SLA).

ג. המערכת תספק מנגנון דיווח ואנליטיקה על כלל התקריות והתהליכים שבוצעו.

ד. המערכת תכלול מנגנון להפקת דוחות אוטומטיים על בסיס KPI ו-METRICS רלוונטיים.

2.1.5. **<u>תשתיות אבטחה למרכז (S) - TSOC</u>**

מערכות אבטחה למרכז הסייבר יספקו הגנה ואבטחה היקפית כמענה לאבטחת מרכז ה TSOC

2.1.5.1. תשתיות אבטחה למרכז תפקידן לספק את האבטחה הראויה למרכז ה TSOC כישות ארגונית אחודה הנשלטת מנוהל ומאובטחת מתוך רשת המרכז בלבד.

2.1.5.2. על הספק לפרט את אופן השילוב של כלל מערכות האבטחה הרלוונטיות לפתרון המוצע על כלל מרכיביהם והקשרים שלהם

2.1.5.3. עבור כל קטגוריה (לדוגמא: "הגנת רשת") וכל מוצר\מערכת בקטגוריה (לדוגמא: "מרכת חומת אש") הספק יפרט את היצרן, את פירוט הרישוי הדרוש, העלות ואופן הניהול

2.1.5.4. על כלל המערכות, המוצעות על ידי המציע, לקיים את רמת האבטחה הנדרשת בהתאם לפרק אבטחת המידע במכרז.

2.1.5.5. על הספק לפרט מערכות מהקטגוריות המובילות (ללא מוצרים נישתיים - (niche players) על בסיס מדד .Gartner (באחד מ-3 הדו"חות האחרונים).

2.1.5.6. הספק יפרט ארכיטקטורת על HLD כחלק משלב א' במכרז ויפרט את קשרי הגומלין בין המערכות + יספק תצורת רשת כוללת לכלל המוצרים תוך שמירה על היבטי אבטחת המידע בפתרון.

2.1.5.7. הספק רשאי לאחד בין מוצרים ושירותים (בתצורת Cloud Native או ספקי SaaS נוספים) ובתנאי כי הפונקציונליות המרכזית המשמשת את המוצר בקטגוריה נשמר בהיבט האבטחה. על הפסק לפרט שילוב של מערכות וכיסוי שמערכות עבור פונקציונליות מרכזית במענה ה HLD וה LLD.

2.1.5.8. התשתיות, השירותים והמערכות יכללו את המוצרים מהקטגוריות הבאות:

הגנת רשת	מערכת חומת אש Firewall ברמת מיקרו-סגמנטציה
	מערכת חומת אש אפליקטיבית Web Application Firewall (WAF)
	מערכת אבטחת ממשקים (API Gateway)
	מערכת DDoS Protection
	מערכת גישה מאובטחת מרחוק SSE
אבטחת מידע	מערכת לזיהוי הימצאות מידע רגיש (DSPM ו-DLP)
	מערכת להעברת קבצים מנוהלת (MFT)
	ניהול מכשירים ניידים (MDM) ואפליקציות (MAM)
פוגענים ונוזקות	מערכת זיהוי ושיקום ברמת מערכות הפעלה, עמדות הקצה וקונטיינרים (Container Runtime, XDR וכד')

	מערכת הלבנת קבצים (CDR + Sandbox)
	ארגז חול פוגענים (Sandbox)
הגנת סביבת ענן	כל המידע והשרתים במערכת צריכים להיות מוצפנים באמצעות מערכת ההצפנה המובנת של ספק הענן (CSP) כאשר ניהול המפתחות בשליטת המציע (CMK).
	פלטפורמה להגנת סביבת הענן ותצורת האבטחה כגון (SSE,CloudDR ,CASB ,CNAPP)
	מערכת ניהול מפתחות וסודות (KMS)
ניטור ותגובה	מערכת ניהול התראות אבטחה מרכזית (SIEM) – (אחודה עם מערכת "על" - SIEM OF SIEM'S)
	מערכת גילוי משטחת תקיפה חיצוני (VAS\EASM)
	מערכת איסוף מודיעין מסחרי (Threat Intelligence)
	מערכת תגובה לאירועים באופן אוטומטי (SOAR) – אחודה עם המערכות התומכות של המרכז)
ניהול זהויות	מערכת ניהול זהויות מרכזית וניטור הרשאות ענן (IDP+IAM+CIEM) מרכזי שיאפשר שליטה על כל הזהויות)

2.1.6. שלב א' - אפיון המערכת. מהות השירות המבוקש (S)

2.1.6.1. יש לפרט ארכיטקטורה מקיפה של הפתרון (HLD, LLD) ושל מוצרים הכלולים בו. בין היתר יש לפרט את התצורה והטכנולוגיה, רכיבי הענן, חומרה ותוכנה, אפליקציות, צורת ואופן ההזדהות, הצפנת המידע, שימוש באמצעים מאובטחים להעברת מידע, מערכות קליטה, סינון וביצוע אנונימיזציה למידע, הקשחות המערכות, אבטחת סביבת הענן, הלבנת מידע נקלט, אמצעי אחסון, ארכיב תוך שימוש בטכנולוגיות מתקדמות המקובלות בשוק ומתן זמינות נתונים ע"פ רמת השרות שתקבע תוך שימוש ב- BEST PRACTICES של ספקי הענן ו- CIS.

2.1.6.2. יש לפרט את כלל ממשקי המערכות אל מול צד לקוח מחד, כולל בין היתר, ניהול הרשאות והזדהויות, גישה ממודרת לתכנים, דוחות כללים, דוחות ספציפיים, התראות בזמן שגרה וחרום, בלוגים וחיבור צ'ט למומחה, תמיכה מאובטחת בהעברת קבצים גדולים, תמיכה בניהול אירועים לפי work flow מובנה, יכולות של הוצאת/הכנסת נתונים למערכות חיצוניות ותמיכה בכל הפורמטים המקובלים: xml, hml ,html ,csv ,excel, pdf וכו'

2.1.6.3. יש לפרט את הטכנולוגיה שמיושמת לצורך ההזדהות חזקה מתן הרשאות, הצפנת תעבורה, ניטור החיבור, MFA, בדיקת תאימות למערכות אבטחה ועדכוני אבטחה.

2.1.6.4. יש לפרט אופן הטמעה והדרכה למשתמשים המיועדים לשלב התפעול של המערכת.

2.1.6.5. יש לפרט את אופן ההצפנה בסביבת הענן, ניהול המפתחות, ניטור, מרכיבי ההגנה ואופן ההגנה על פי BEST PRACTICE של ספק הענן ו- CIS.

2.1.6.6. יש לפרט תמיכה טכנית למערכות: תחזוקה, שינויים ושיפורים.

2.1.6.7. יש לפרט תהליכי בדיקות של התשתית, הפונקציונאליות והאבטחה (עמידה רלוונטיות בתקנים וכ"ו).

2.1.7. דרישות מנהלתיות

2.1.7.1. הספק יתכנן מראש ויספק בהתאם לצורך:

2.1.7.1.1. **<u>אספקת ציוד מחשוב למרכז ה TSOC:</u>** קווי אינטרנט וציוד תקשורת למרכז TSOC, מחשבים ניידים חזקים ומתקדמים לאנשי צוות ההקמה + אנשי צוות התפעול, עמדות עגינה, 2 מסכים לכל בעל תפקיד המוצע על ידי הספק, ציוד מחשוב היקפי, ציוד מולטימדיה

(מסכי תצוגה, מקרנים, עמדות KVM מאובטחות), טלפוניית IP מאובטחת למרכז, מכשיר סלולרי המשמש את המרכז + חבילת סלולר.

2.1.7.1.2. **<u>אספקת ערכות חיבור לג"מים:</u>** ציוד ותשתיות רלוונטיות בהתאם לאפיון הארכיטקטורה של הספק שאושרה על ידי המזמין.

2.1.7.1.3. **<u>אספקת ציוד משרדי למרכז</u>**: שולחנות עבודה, כיסאות, עמדות עבודה בעמידה, ציוד משרדי.

2.1.7.1.4. **<u>אספקת ציוד מעטפת</u>**: ציוד מטבח - מקרר, מיקרוגל, טוסטר, קומקום, מכונת קפה, ציוד חד פעמי, כוסות קפה + קפסולות\פולי קפה.

2.1.7.1.5. תקציב קופה קטנה חודשית לאספקה למזון למשמרות ערב ולילה עבור עובדי המרכז וכיבוד קל עבור מבקרי המרכז.

2.1.7.1.6. התקשרות עם גב-ים / מתחם ה SOC-עבור שתי חניות להנהלת מרכז הניטור ושתי חניות עבור משרד התחבורה.

2.1.8. **שלב א' – שירותים אופציונאליים נוספים (G)**

2.1.8.1. מתן שירותי מודיעין סייבר – כדוגמת כלי OSINT, איסוף וניתוח תמונת מודיעין הן ע"י כלים ייעודיים והן ע"י מקורות חיצוניים (צד שלישי או מקורות נוספים).

2.1.8.2. התממשקות למקורות מידע אבטחתיים רלוונטיים בתחום פלטפורמות תחבורה חכמות באוויר בים וביבשה.

<u>מוצרים נוספים שהמציע יספק (אופציונלי)</u>

2.1.8.2.1. רישוי למודיעין מסחרי עבור 50 גופים.

2.1.8.2.2. מערכת סריקת חולשות פרו אקטיבית ל-50 גופים.

2.2. שלב ב'- הקמת מרכז שליטה ובקרה (TSOC) ומערכת שו"ב לגיבוש תמונת מצב מגזרית, איתור, ניהול, תחקור, ניתוח והתאוששות מאירועי סייבר

2.2.1. מטרת שלב ב' (I)

2.2.1.1. הרחבת האפיון שבוצע בשלב א' כפי שזה הוגש למשרד ותכנון מימוש מלא של המרכז TSOC על בסיס האפיון, כולל התקנת מערכות, אינטגרציה, בדיקות תקינות והרצת מערכות.

2.2.2. דרישות (M)

2.2.2.1. **<u>חלק ב'1 – פיתוח יכולות המרכז ובדיקות קבלה</u>**

2.2.2.1.1. במסגרת שלב זה יבצע הספק שיפור והתאמות נדרשות לאפיון המוצע משלב א' בהתאם להערות שיקבל מהמשרד.

2.2.2.1.2. הספק יבצע את כלל ההתאמות והדיוקים לאפיון שבוצע בשלב א' הן בשלב תפיסת ההעלה והן ברמת האפיון הטכנולוגי.

2.2.2.1.3. הספק יחל בהקמת תשתיות הענן בסביבה ייעודית עבור המשרד – על ידי צוות ההקמה.

2.2.2.1.4. פריסת מערכת העל Siem Of Siem's.

2.2.2.1.5. פריסת מערכות כלל המערכות, התשתיות והשירותים המשמשים את תשתיות השו"ב המרכזית של מרכז ה TSOC וביצוע האינטגרציה עם כלל המערכות במרכז.

2.2.2.1.6. אינטגרציה בין מערכות השו"ב לתשתיות עם מערכות קיימות.

2.2.2.1.7. פיתוח אוטומציות לתהליכים מבצעיים ובפיתוח חוקים וחוקות ראשוניות.

2.2.2.1.8. הקמת המרכז בהיבט הפיזי, בכולל פריסת תשתיות מחשוב ותקשורת, שילוב מערכות בפן הפיזי במרכז באתר המרכזי ובאתר הגיבוי שיוגדר על ידי המשרד.

2.2.2.1.9. פיתוח, דיוק וכתיבת תפיסת ההפעלה מעודכנת שתשמש את צוות ההפעלה המבצעית, הנהלים והמסמכים בהתאם למצב בפועל As Made של מרכז ה-TSOC.

2.2.2.1.10. **<u>ניהול תהליך הבדיקות</u>**

2.2.2.1.10.1. באחריות המציע לנהל במלואו את כל תהליך ביצוע הבדיקות עבור כל מערכת המרכז, בהתאם לאישור מפרט הבדיקות שיאושר על ידי המשרד.

2.2.2.1.10.2. המציע נדרש לבצע, ככל הניתן, את הבדיקות באופן אוטומטי וממוחשב לטובת יכולת תיעוד וביצוע חזרתי, מהיר, יעיל ומהימן.

2.2.2.1.10.3. במסגרת ניהול הבדיקות יבצע המציע את הפעילויות הבאות:

א. אישור הצורך בבדיקה מול המשרד

ב. תכנון הבדיקות, הכנת מסמכי הבדיקות ואישור מסמכי הבדיקות במסגרת סקר בדיקות TRR.

ג. ניהול זמניות וכשירות המרכז לצורך ביצוע הבדיקות כולל מתארי בדיקה וציוד.

ד. ניהול האמצעים לביצוע הבדיקות: ציוד, משאבים כח אדם וכו'.

ה. תיאום צוות הבדיקות של המשרד לביצוע הבדיקות.

ו. ניהול תהליך הבדיקה – שלבי התהליך, מעבר לנוהל כשלון, מתודולוגיית רישום ותיעוד וכו'

ז. הפקת מסמכי תוצאות בדיקה והעברתם לאישור המשרד

2.2.2.1.11. **<u>נוהל ביצוע הבדיקות</u>**

2.2.2.1.11.1. הבדיקות יבוצעו ע"י המציע בנוכחות ופיקוח אנשי המשרד או נציגים שיוסמכו לכך ע"י המשרד.

2.2.2.1.11.2. הבדיקות יבוצעו בהתאם למפרטי הבדיקות המאושרים ב- TRR.

2.2.2.1.11.3. במהלך ביצוע הבדיקות יירשמו תוצאות הבדיקה באופן מפורט ומלא.

2.2.2.1.12. **<u>נוהל סיכום בדיקות:</u>**

2.2.2.1.12.1. לא יאוחר מ-5 ימי עבודה מסיום הבדיקות יעביר הזכיין למזמין דו"ח תוצאות מודפס וחתום על ידי מנהל הבדיקות.

2.2.2.1.12.2. דוח תוצאות הבדיקה יכיל לפחות את הנושאים הבאים:

א. סעיף יחוס במסמך הדרישות ותיאור הבדיקה.

ב. ניתוח תוצאות הבדיקה אל מול תוצאה נדרשת.

ג. קביעת הצלחה/כשלון של הבדיקה.

ד. ליקויים שנתגלו במהלך הבדיקות ולו"ז לתיקונם.

ה. הערות ומסקנות.

2.2.2.1.13. **<u>נוהל כשלון בדיקות</u>**:

2.2.2.1.13.1. המציע ידווח מיידית לגורמי המשרד על כשלון בדיקה.

2.2.2.1.13.2. בכל מקרה של כישלון, המציע מתחייב לתקן את הליקויים לשביעות רצון המשרד, תוך פרק זמן המבטיח עמידה בלו"ז הפרויקט.

2.2.2.1.13.3. לאחר תיקון הליקויים המציע יחזור על ביצוע הבדיקות עצמן וגם על כלל הבדיקות אשר עשויות להיות מושפעות מאותם ליקויים, ללא תמורה נוספת.

2.2.2.1.13.4. דו"ח הבדיקות יכלול בנוסף את פירוט הפעולות שננקטו לתיקון הליקויים ומהותם.

2.2.2.2. **<u>חלק ב'2 – הרצת מערכת ראשונית כפיילוט על גופים נבחרים:</u>**

2.2.2.2.1. בשלב זה יכניס הספק את הצוות ביצוע POC אשר יבוסס על "צוות ההקמה" בשילוב אנשי "צוות ההפעלה המבצעית" לצורך ביצוע חפיפה בין צוות הקמה לצוות ההפעלה המבצעית על כלל המערכות והכלים וביצוע תהליך הבדיקה מקצה לקצה בהתאם ל Use Cases שיוגדרו על ידי המשרד הספק ויאושרו על ידי המשרד.

2.2.2.2.2. תבוצע הפעלה של כלל המערכות ותבוצע בדיקת שפיות לתהליכי העבודה הפנימיים כולל בדיקה של קיום תהלכים מתפיסת ההפעלה, אוטומציות, התראות, דיווחים, שילוב של גורמים אנושיים ואנשי קשר מהמשרד, מהמרכז TSOC ומהג"מ.

2.2.2.2.3. הספק יבצע חיבור של 4-5 ג"מים מתועדפים לאינטגרציה עם מערכות המרכז על פי הפתרון המוצע על ידי הספק.

2.2.2.2.4. יבוצעו בדיקות תקינות המרכז בהתאם למסמך KPI שייכתב על ידי הספק, יאושרו וייבדק בשיתוף עם נציג המשרד - הערכת ביצועים והתאמות לשיפור התפקוד של המרכז.

2.2.3. **שלב ב' - מהות השירות המבוקש (S)**

2.2.3.1. הספק יפרט את שלבי ההקמה בהתאם לעמידה בלו"ז הפרויקטלי.

2.2.3.2. הספק יבצע רכש תשתיות, מערכות ומוצרים ויחל בתהליך השילוב במרכז ה TSOC.

2.2.3.3. יבוצע תיעוד מפורט של התצורה והטכנולוגיה, רכיבי הענן, חומרה ותוכנה, אפליקציות, צורת ואופן ההזדהות, הצפנת המידע, שימוש באמצעים מאובטחים להעברת מידע, מערכות קליטה, סינון וביצוע אנונימיזציה למידע, הקשחות המערכות, אבטחת סביבת הענן, הלבנת מידע נקלט, אמצעי אחסון, ארכיב ומפרט של כלל התשתיות המערכות ואפיון המערכות.

2.2.3.4. בתום שלב פיתוח המרכז ובמקביל לשלב מבחני הקבלה יבצע הספק בדיקות חדירות על כלל התשתיות והמערכות

ידי ספק חיצוני בלתי תלוי שיאושר על ידי המשרד. בנוסף יבצע הספק סקר סיכוני סייבר ובדיקת רמת יישום בקרות SECURITY MATURITY LEVEL על כלל המערכות והתשתיות של המרכז.

2.2.3.5. הספק יבצע את תיקון כלל הליקויים והפערים שיעלו במסגרת מבחני הקבלה, בדיקות החדירות והפערים שיעלו בסקר הסיכונים ליישום רמת הבקרה SML על חשבון הספק.

2.2.3.6. הספק יבצע הרצה של כלל המערכות ויחל בהכשרת צוות ההפעלה המבצעית.

2.2.3.7. באחריות הספק לבצע את כלל הפעולות להשלמה מוצלחת של ה POC ועמידה בכלל ה KPI וה USE CASES בהתאם ללו"ז הפרויקטלי.

2.3. **שלב ג' – מוכנות להפעלה.**

2.3.1. **מטרת שלב ג' (I)**

2.3.1.1. מטרת השלב לעבור משלב ההקמה ושלב התפעול השותף ולמבצוע המרכז, המערכות וכח האדם הקבוע לתפעול המרכז TSOC

2.3.2. **דרישות – שלב ג' (M)**

2.3.2.1. **<u>חלק ג'1 – הטמעת ג"מים – חיבור כלל הג"מים למערכות מרכז ה-TSOC.</u>**

2.3.2.2. כחלק מתהליך שילוב הג"מים יבצע הספק שילוב מדורג מתוכנן ומתואם עם המשרד לשילוב כלל מקורות המידע במערכות ה TSOC.

2.3.2.3. כחלק משלב זה יידרש הספק לתגבר את צוות התשתיות והאינטגרציה לחיבור כלל הג"מים בהתאם לאבני הדרך של הפרויקט

2.3.2.4. **<u>חלק ג'2 – מבחני קבלה למבצוע המרכז – מעבר המרכז למבצעיות בכלל ההיבטים כמרכז ה TSOC-של המשרד.</u>**

2.3.2.5. כחלק משלב זה יידרש הספק לבצע העברת אחריות מלאה "מצוות ההקמה" ל"צוות ההפעלה המבצעית" בתצורת "שולחן

נקי" כאשר כלל משימות האינטגרציה, הטמעה הטיפול בתקלות ופערים נסגר על ידי צוות ההקמה.

2.3.2.6. על הספק בשלב זה לספק תמונת במצב רוחבית מתוקפת על מצב משק מגזר התחבורה במדינת ישראל ומשלב זה להתחיל את שלב התפעול השותף.

2.3.3. **שלב ג' - מהות השירות המבוקש (S)**

2.3.3.1. הספק יבצע טיפול השלמת כלל הפערים משלב ההקמה ויוודא תקינות ופעילות מבצעית של כלל המערכות כולל חיבוריות תקינה לג"מים.

2.3.3.2. הספק יבצע "העברת מקל" בין צוות ההקמה "לצוות ההפעלה המבצעית" ויחל את שנת הבדק.

2.4. **שלב ד' – הפעלה -** מעבר של המרכז משלב ה POC לשלב מבצעי בו מחוברים למרכז כלל הגופים המוגדרים על ידי המשרד.

3. אבטחת מידע

3.1.1. **כללי (I)**

דרישות אבטחת המידע במערכות שיוקמו לטובת המרכז TSOC יתבססו על תקנים הבאים:

א. ISO/IEC 27001 – תקן ניהול אבטחת מידע, המגדיר מסגרת לניהול מאובטח של נתונים ומידע בארגון.

ב. ISO/IEC 27017 – תקן המרחיב את ISO 27001 עם בקרות אבטחת מידע לסביבות ענן.

ג. ISO/IEC 27018 – תקן ספציפי להגנה על מידע אישי (PII) בשירותי ענן.

ד. NIST CSF 2.0 (Cybersecurity Framework) – מסגרת לניהול אבטחת סייבר של ארגונים, כולל משילות, זיהוי, הגנה, זיהוי איומים, תגובה והתאוששות.

ה. הספק יציג עמידה במתודות "ניהול סיכונים בחברות שרשרת אספקה" של מערך הסייבר הלאומי בתוך שנה מהזכייה במרכז.

ו. המציע מתבקש לפרט את פתרונו המוצע בהקשר של אבטחת מידע ע"פ עקרונות CIA ובהתאם לנספח ד' ולעקרונות המנחים הבאים שמטרתם להבטיח הגנה על נכסי המידע המסווג של המשרד:

- **CONFIDENTIALITY** – <u>חשאיות וסודיות המידע</u>: המידע חשוף ונגיש רק למי שקיבל הרשאת גישה.
- **INTEGRITY** – <u>אמינות ושלמות המידע</u>: דיוק ושלמות של המידע ושל שיטות עיבוד המידע. כלומר לא בוצע שינוי במידע שלא באישור ובסמכות של בעל המידע.
- **AVAILABILITY** – <u>זמינות ונגישות המידע</u>: מערכת נגישה למשתמשים המורשים בזמן הנדרש.

3.1.2. אבטחת מידע במוצרי SaaS

אבטחת המידע במערכות שיוקמו לטובת המרכז TSOC בתצורת SaaS יציגו עמידה בדרישות הבאות

א. עמידה בתקני אבטחה בינלאומיים - המוצר מתקשר להציג ביקורת בלתי תלוייה עם תקני ISO 27001 ו- SOC 2 Type - - יוצגו אישורים והוכחות בהתאם להסמכות.

ב. עמידה בדרישות החוק להגנת הפרטיות הישראלי IPPL או לחלופין GDPR.

ג. מיקום המידע – המידע של המערכת יהיה באזור המשילות הישראלי אצל ספק תשתיות ענן GCP ו AWS בהתאם להגדרות אבטחת המידע בפרויקט "נימבוס".

ד. הצפנת המידע – הספק יציג עמידה בהצפנת מידע תנועה ובמנוחה בהלימה לתקני הצפנה לכל הפחות בהתאם לדרישות FIPS140-2.

ה. הצהרה כי הספק אינו מאפשר למודלי AI מבוססי - LLMs להתאמן או לשמור מידע על של הלקוח במערכות אלו.

ו. הצהרה של הספק לניהול תהליכי ניטור ואבטחה, קיום נהלי תגובה ועדכון לקוחות בעת אירוע סייבר, ניהול סיכונים בשרשרת אספקה.

ז. הספק יצהיר את כלל מעבדי המידע המשניים (Data Subprocesses) איתם הוא חולק את המידע. – הנ"ל לא יגרע מדרישות משילות המידע.

3.1.3. סקרי סיכונים, ביקורות ומבדי חוסן (M)

- **<u>בדיקות חוסן</u>** - הספק יבצע בדיקות חדירות על כלל התשתיות והמערכות (אפליקטיבית ותשתיתית) 2 פעמים בשנה (בכל שנת

הפעלה לרבות שנות האופציה) על ידי ספק חיצוני בלתי תלוי. הספק החיצוני וסקופ הבדיקה יאושרו על ידי המשרד.

- **<u>סקר סיכונים</u>** – הספק יבצע פעם בשנה (לרבות תקופות האופציה) סקר סיכוני סייבר ויציג את ממצאי הסקר למשרד, דו"ח ליקויים ותכנית תיקון הליקויים. הסקר הראשון יתקיים כחלק מתהליך האפיון והקמה.

3.1.4. **סיכוני אבטחת מידע - דוגמאות (I)**

- חשיפת מידע מסחרי רגיש, לוגים ותחקירים של אירועים אמיתיים.
- פריצה למרכז TSOC ושתילת תכנים זדוניים.
- שינוי מידע רגיש אשר מגיע למרכז TSOC המאובטח או למערכת השו"ב.
- העברת פוגען למרכז ה TSOC או אל ג"מ או להפך והפצתו במגזר כולו.
- העברת פוגען ממערכת ה- SIEM'S OF SIEM'S אל ג"מ או להפך והפצתו במגזר כולו.
- שיבוש / השבתה / פגיעה בפעילות שוטפת של גוף/ים מונח/ים.

3.1.5. **ניהול משתמשים, זהויות והרשאות (M)**

ניהול זהויות וגישה לאזורים ממודרים כחלק מפתרון השתלטות וגישה מאובטחת מרחוק לצורכי עבודה ותחזוקה –תתאפשר גישה מאובטחת דרך האינטרנט שתעבור מספר שלבים מבוקרים כתלות בפרופיל המשתמש, ברמת סיווגו ובמידע הנדרש. להן תיאור השלבים העיקריים:

3.1.5.1. גישה מאובטחת למרכז TSOC באמצעות certificate חוקי ומאושר.

3.1.5.2. Multi Factor Authentication בגישה למרכז הTSOC ולכלל המערכות.

3.1.5.3. **מידור:**

החומרים צפויים להגיע משותפים שונים ומגוונים. ייתכן שהחומרים יהיו ברמות רגישות שונות. לשם כך על המערכת להבטיח הפרדה מלאה בין סוגי החומרים והמשתמשים השונים ולאפשר מתן הרשאות מדויקות Need To Know ברמת דיוק (גרנולריות) לכלל המשתמשים והתהליכים במערכות המרכז:

- הרשאות לדוגמא: צפייה מאובטחת (ללא יכולת הורדה),כתיבה, קריאה, עריכה, חיפוש, פירוט החומרים במאגר ועוד.

- הגבלת גישה – מכתובות IP, מיקומים גיאוגרפיים, שעות, ממשקים וכ"ו.

3.1.5.4. **ניהול סיסמאות:**

- על כלל הסיסמאות המנוהלות במערכת להיות שמורות במאגר ייעודי ומאובטח.
- הגישה לסיסמאות תהייה ע"פ הרשאה ספציפית וכן תהייה הפרדה מלאה בין ניהול ותוכן כלומר מנהל התשתית לא יהיה חשוף למידע השמור במערכות.
- זיהוי סיסמאות פריווילגיות באופן אוטומטי כולל הגדרה אוטומטית במערכת.
- הרשאת גישה למשתמשים בהתאם להיררכיה ב IDP או היררכיה מוגדרת באופן ספציפי.
- מנגנון להחלפת סיסמאות ע"פ מדיניות בארגון.
- מנגנון חידוש סיסמא למשתמשים
- תמיכה במספר מדיניות (POLICIES) המוגדרות מראש.

3.1.5.5. **תמיכה בתשתיות:**

- תמיכה בהזדהות חזקה MFA.
- אפשור גישה לכלל הרכיבים הקיימים ברשת כגון שרתים, התקני אכסון, התקני תקשורת, ממשקים WEB תתבצע מתוך רשת מרכז ה TSOC בלבד ולא מכתובת ברשת האינטרנט.

3.1.5.6. **ניהול משתמשים**

- מתן הרשאות גישה עפ"י פעולה ולא רק עפ"י המשאב.
- תמיכה בהגדרת תפוגה למשתמשים.

3.1.5.7. **יכולת: analytics**

- יכולת ייצור התראות בזמן אמת על שימוש חריג במערכת.
- קבלת מידע מליבת המערכות במרכז ה TSOC למערכת ה SIEM והפקת התראות ייעודיות למרכז ה TSOC.

3.1.5.8. **יכולת: audit**

- תיעוד מלא של השימוש בהרשאות, בתשתיות ובמערכות השונות של מרכז ה TSOC.
- תיעוד מלא של פעולות המתבצעות באמצעות ההרשאות.
- השתלבות עם מוצרי SIEM לצורך תחקור אירועים.

3.1.5.9. **non-repudiation (אי הכחשה)**

- כל הפעילות במערכת צריכה להיות מנוטרת באופן שאינו מאפשר התערבות, מחיקה או הכחשת ביצוע (TEMPER PROOF LOG).

3.1.5.10. **יכולת חיפוש אירועים וניתוחם**

- יכולת חיפוש אירועים ע"פ מילות מפתח
- ניתוח METADATA

3.1.5.11. **יכולת אכיפה**

- SINGLE POINT OF CONTROL
- ממשק ניהול אחוד.

3.1.5.12. **ניהול סיסמאות אפליקטיביות**

- מימוש ניהול סיסמאות אשר שמורות בתוך קטעי קוד של אפליקציות על בסיס Token זמני מנוהל באופן מרכזי.
- זיהוי חזק של אפליקציות הניגשות למאגר הסיסמאות עבור סביבת מרכז ה TSOC.
- ניהול סיסמאות אפליקטיביות בהתאם למדיניות שתיקבע.
- תמיכה בניהול סיסמאות בשימוש שרתי אפליקציה.

ניהול גישת המשתמשים למרכז ה TSOC הנו באחריות מנהל הפרויקט (בשלב ההקמה) ומנהל המרכז (בשלב ההפעלה המבצעית) שיוגדר לשם כך בפרויקט. המציע ידריך, ילווה ויטמיע את הגדרת המשתמשים.

3.1.6. **ניהול תווך מאובטח (M)**

3.1.6.1. **תווך מאובטח:**

- כחלק מפתרון השתלטות וגישה מאובטחת מרחוק לצורכי עבודה ותחזוקה יתבצע שימוש במערכת SSE - SECURE SERVICE EDGE .
- על הפתרון המוצע לייצר חציצה בין עמדת המשתמש לתשתית, קיום בידוד מלא של רכיבי התשתית.
- נדרשת שליטה מלאה בתווך כגון : שעות פעילות, IP, מיקום גאוגרפי, כולל צפייה בזמן אמת והתערבות במידה הצורך בזמן החיבור הפעיל.
- יכולת הקלטת החיבור המאובטח באופן רציף וללא השפעה על רכיב הקצה – עבור גישה לניהול התשתיות.
- על ההקלטות להישמר במאגר מאובטח ונדרשת בקרת גישה למידע.
- נדרשות יכולות חיפוש בתוכן ההקלטות.
- נדרשת תמיכה בהתחברות לכל סוגי התשתית וכן לכלל ממשקי הניהול והתפעול של המערכות.

3.2. **אתר הגיבוי והתאוששות מאסון של ה-TSOC (S)**

האתר המשני ישמש עבור התפקידים הבאים:

3.2.1. <u>בזמן שגרה</u>: ישמש כאתר גיבוי פושר לאתר הראשי.

3.2.2. <u>בזמן חרום</u>: ידלג צוות התפעול באתר הראשי אל אתר הגיבוי שיהפוך בשעת חרום, לתפקד כאתר הראשי של ה-TSOC.

בהמשך לסעיפים שלעיל, יש לפרט ולציין כיצד תובטח הזמינות הגבוהה, השרידות והביצועים של המערכת ברמת זמינות השרות של 99.0% תפקוד בשנה:

- הפסקת שרות של עד: 3.65 ימים בשנה; או
- הפסקת שרות של עד: שהם 7.20 שעות בחודש; או,
- הפסקת שרות של עד: שהם 1.68 שעות בשבוע.

כן יש לפרט מהם זמני ההתאוששות הצפויים למערכת כולה על כל אחד מרכיביה השונים:

- RTO - (Recovery Time Objective
- RPO – (Recovery Point Objective)

4. טכנולוגיה, תשתית, אתר גיבוי והתאוששות וכח אדם מקצועי לתפעול המערכת (S)

בכל מקרה בו קיים מכרז מרכזי מתאים (לציוד או לתוכנה) מטעם החשכ"ל במשרד האוצר, הרכיבים יותאמו לפי מכרז החשכ"ל המתאים, גם אם הציוד או התוכנה לא יהיו זהים לגמרי לאלו שהמכרז המרכזי האמור.

4.1. ארכיטקטורה (I)

4.1.1. **<u>האתר הראשי (Production Site)</u>** באתר שיוקצה ויוגדר על ידי המשרד, יכלול את המערכות והמרכיבים הבאים (בעת פרסום המכרז כוונת המשרד להקים את ה SOC-במתחם ה SOC-הלאומי במערך הסייבר בבאר שבע, אך ניתן לשינוי ע"י המשרד):

- חדר אירוח ציוד תקשורת ממוגן ברמת Tire-2 לפחות. (מקור ראשי, מקור משני (גנראטור) וגיבוי UPS למקרה שהמקור המשני נכנס לפעולה באופן מידי).
- איוש המרכז: המרכז יפעל 24/7 במתכונת משמרות יום, ערב ולילה. שעות פעילות
  - שעות פעילות יום: 07:00-16:00
  - משמרת ערב 16:00 – 23:00
  - משמרת לילה: 23:00 עד 07:00 למחרת
- מרכז ניטור אבטחת סייבר - (TSOC) בחלל זה ימוקם ה- TSOC אותו יאיישו בשעות הפעילות: 2 -בקרי סייבר במשמרת יום ואילו במשמרת ערב ולילה בקר סייבר אחד , ר"צ\אחמ"ש במשך משמרת היום. אנליסט T3 במשמרת יום, מנהל ה TSOC-ישב בחדר צמוד ל TSOC-ויאויש ביום, צוות התשתיות והאינטגרציה ישב בחדר צמוד ל TSOC-ויאויש ביום.

4.1.2. **<u>האתר המשני (Backup Site & Worm Disaster Recovery)</u>** ישמש כאתר גיבוי פעיל - Active Active לא מאוייש בשגרה ויתפקד כאתר דילוג במקרה אסון – DRP צוות ה

TSOCידלג לאתר זה ע"פ הגדרת תוכנית ההמשכיות העסקית
שתוגדר למרכז. מיקומו הפיזי של אתר המשני יוגדר ע"י המשרד.

4.2. כוח אדם מקצועי (I)

כח האדם שיעסיק הזוכה יהיה בהעסקה ישירה ובאחריותו הישירה של הזוכה (שכר, נסיעות, הסעדה, חופשים, הזנה, הפרשות סוציאליות וכו') באופן שיהלום למול תנאיהם של עובדים מקבילים במרכז ה SOCהלאומי. יחד עם זאת, המזמין שומר לעצמו את הזכות, לפי שיקול דעתו הבלעדי, לגייס כ"א מטעמו לצורך מתן השירותים נשוא מכרז זה – כולם או חלקם – וזאת באמצעות הליך תקני בהתאם למכרז כ"א של חשכ"ל. ככל שייעשה שימוש בכ"א מטעם המזמין, יפעל הספק הזוכה בהתאם להנחיות שייקבעו, לשם שמירה על רציפות תפעולית, הכשרה, שיתוף מידע ואחידות תהליכי העבודה במרכז ה) TSOC-למען הסר ספק, במקרה זה, הספק לא ידרוש תשלום על כ"א המוחלף על ידי המזמין באמצעות מכרז חשכ"ל).
הצוות שיעמיד הזוכה לטובת המרכז יהיה ייעודי עבור מרכז ה TSOC ויכלול את הצוותים הבאים:

4.2.1. <u>צוות ה TSOC</u>

4.2.1.1. בקר\ית סייבר (T1) – 2 משרות במשמרת יום ו-משרה 1 במשמרת ערב ולילה במשמרות 7\24 (היערכות הספק לכ"א בהתאם לתחלופת משמרות)

סינון וסיווג ראשוני, העשרה טכנית, פעולת תחקור ואנליזה בסיסיות של אירועים, פתיחה ותיוג אירוע במערכת, מתן המלצות לטיפול בהמשך, דיווח לאנליסט ותגובה ראשונית למתקפה ו/או איום.

4.2.1.2. ר"צ / אחמ"ש (T2) – משרה 1 באיוש משמרת יום בלבד 5 ימים בשבוע

סינון וסיווג מעמיק, העשרה וניתוח טכני, פעולת תחקור ואנליזה כולל הרצת כלים מתקדמים על אירועים, אבחון וניתוח מגמות, יצירת תמ"צ, דיווח מול גורמים נוספים וחיצוניים למערכת, טיפול וניהול אירועים מתגלגלים, דיווח/התייעצות עם אנליסט בכיר, מתן המלצות לבקרים במגזר והמשך הטיפול, סגירת אירוע המערכת.

4.2.1.3. אנליסט\ית בכיר\ה – (T3) משרה 1 באיוש משמרת יום בלבד 5 ימים בשבוע.

פיתוח יכולות המרכז ומערכות הניטור, דיוק החוקים, הקמה מתודולוגית של יכולות ניטור ייעודיות למרכז, משתמש על של מערכת ה SIEM וערכות השו"ב המרכזיות שיוקמו למרכז.
ביצוע פעולות ניתוח מתקדמות, REVERSE ENGINEERING, מחקרים עמוקים ויזומים, הוצאת המלצות להתמודדות כנגד פוגענים, פרסום מאמרים על איומים במגזר וניתוח פוגענים,

הצלבת מידע מול מגזרים שונים, מקורות שונים ועבודה עם מומחי סייבר במגזר ומחוץ למגזר.

4.2.1.4. **מנהל\ת ה- TSOC – משרה 1 באיוש משמרת יום בלבד 5 ימים בשבוע.**

אחראי\ת על תפעולו ותפקודו השוטף של ה- TSOC, על תקינות ועדכונים של המערכות, סידורי המשמרות וכוח האדם במשמרת, מהווה סמכות מנחה לתיעדוף וניהול אירועים, כוח אדם לטיפול באירוע בחמ"ל, אחריות למעבר ממצב שגרה לחרום ולהיפך, אחרי על הדיווח והאסקלציה אל מול דרג מקבלי ההחלטות במגזר.

4.2.1.5. **מנהל\ת אדמיניסטרטיבית – משרה 1 על תקן חצי משרה 5 ימים בשבוע.**

אחראי\ת על ניהול המשימות האדמיניסטרטיביות של מנהל ה- TSOC. (ניתן לתמחר כשרות).

4.2.1.6. **מנהל התשתיות בכיר של מרכז ה- TSOC – 1 תקן באיוש משמרת יום בלבד 5 ימים בשבוע.**

אחראי על ניהול כלל התשתיות של המרכז TSOC ומתן שירות ותמיכה לחיבור, תפעול ותקלות בקישורים לג"מים – בעל הרשאות גבוהות לניהול כלל התשתיות כ ADMIN המערכות.

4.2.2. **צוות משלים למרכז ADD-HOC**

4.2.2.1. **צוות IR תחקור אירוע בזמן אמת** – צוות של **2 מומחים בהפעלה על פי דרישה על בסיס בנק שעות של 1000 שעות בשנה + שעות הרחבה על פי דרישה**

זמינות הצוות לקריאה תוך 4 שעות מגילוי האירוע ע"י מנהל מרכז ה TSOC לטובת טיפול באירועים בג"מ ו/או מרגע זיהוי האירוע במרכז או על פי דרישה של הג"מ. הצוות יעבוד על פי נוהל עבודה מוגדר שיאושר על ידי המשרד. הצוות ישמש גם כצוות תחקור אירוע לאחר מקרה – תחקור אירוע לאחר זיהוי, תחקור מקורות התקיפה מהות התקיפה, מודיעין ומתן הנחיות לגופים. הצוות יעבוד על פי נוהל עבודה מוגדר שיאושר על ידי המשרד. הצוות ייחבר רק מאחת החברות בפרויקט "MIRROR" של מערך הסייבר.

4.2.2.2. **צוות תשתיות + אינטגרציה** – צוות של **2 מומחים בהפעלה על פי דרישה על בסיס בנק שעות של 1000 שעות בשנה + שעות הרחבה על פי דרישה**

הצוות יתפקד כתוספת כ"א על פי דרישה והתשלום על פי ביצוע בפועל של פעילות שתוגדר על ידי מנהל התשתיות הבכיר של

מרכז ה TSOC לצורך מתן שירותי תמיכה לחיבור, תפעול ותקלות בקישורים לג"מים.

4.3. **הכשרת כח אדם** – המציע יוודא ויממן כשירות ויספק את כלל ההכשרות הרלוונטיות לעובדים על פי דרישת התפקיד השונות ובהתאם לתיאום ולהנחיית המשרד. המציע יבצע הכשרות תקופתיות מתקדמות שיכללו קורסים מקצועיים, הסמכות לתעודות מקצועיות לבעלי התפקידים השונים (בהתאמה) ותתקצב השתתפות ב -Webinar ים וכנסים מקצועיים לצורך שמירה על כשירות מקסימלית.

4.4. **סיווג ביטחוני** – על כלל העובדים במרכז ה TSOC להיות בעלי הכשר ביטחוני לרמה -3 לפחות שיבוצע על חשבון המציע בהתאם לדרישות קצין הביטחון.

4.5. **תפעול המערכת – (I)**

4.5.1. לצורך הפעלת מרכז ניטור אבטחת סייבר (TSOC) ומערכת שו"ב לניהול, תחקור, ניתוח והתאוששות מאירועי סייבר ושלב ב' בפרויקט נדרש כח אדם מקצועי הכולל את התפקידים הבאים:

4.5.1.1. **בקר סייבר + ר"צ \ אחמ"ש (מקביל לתפקיד בהתאם להוראת תכ"מ 16.2.11 - מקצוע 3.7 - בקר מערכות שליטה ובקרה רמה ב' ו-ג')**

<u>תיאור התפקיד</u>: מתחזק מערכות אבטחת מידע בארגון בהתאם למדיניות הארגון ולהנחיית מנהל אבטחת המידע של הארגון/מערכת.

<u>דרישות התפקיד</u>:

- הנדסאי/ת או טכנאי/ת או סטודנט/ית במקצועות טכנולוגים, לאחר לימודים של שנתיים לפחות באישור מוסד מוכר ע"י המועצה להשכלה גבוהה.
- ניסיון מקצועי בתשתיות תקשוב, אבטחת מידע ומערכות בקרה;
- יתרון לבעלי הכשרה וניסיון בתחומים הבאים: מערכות אבטחת מידע וסייבר בתחום התחבורה ופלטפורמות התחבורה החדשות
- יוזמה אישית; יכולת לימוד ועבודה עצמאית ובצוות;
- יכולת עבודה תחת לחץ ועמידה בלוחות זמנים
- התפקיד עשוי לכלול עבודה במשמרות, כולל סופי שבוע וחגים.

4.5.1.2. **אנאליסט T3 (מקביל לתפקיד בהתאם להוראת תכ"מ 16.2.11 - מקצוע 6.6 -חוקר סייבר רמה ב')**

<u>תיאור התפקיד</u>: בעל הכשרה נרחבת במערכות מחשוב ובאבטחת מידע ומדיסציפלינות שונות, הכרת כלים

מתקדמים לחקירת פוגעניים, יכולת ניתוח פורנזיות וניסיון בתחום התקשורת, מערכות IT, אבטחת מידע וסייבר.

<u>דרישות התפקיד:</u>

- בעל תואר ראשון, לכל הפחות, בהנדסה או מתמטיקה או פיסיקה או סטטיסטיקה.
- חשיבה אנליטית, ידע בשיטות תקיפה וניצול פגיעויות במערכות הפעלה ידע עמוק בתקשורת
- היכרות עמוקה עם מתודולוגיות תגובה לאירועי אבטחת מידע.
- היכרות עם מערכות SIEM;
- יכולת עבודה תחת לחץ ועמידה בלוחות זמנים;

4.5.1.3. **מנהל הTSOC-(מקביל לתפקיד בהתאם להוראת תכ"מ 16.2.11 - מקצוע 6.6 - חוקר סייבר רמה ג')**

<u>תיאור התפקיד:</u> אחראי על תפעולו ותפקודו השוטף של ה-TSOC, על תקינות ועדכונים של המערכות, סידורי המשמרות וכוח האדם במשמרת, מהווה סמכות מנחה לתיעדוף וניהול אירועים, כוח אדם לטיפול באירוע בחמ"ל, אחריות למעבר ממצב שגרה לחרום ולהיפך, אחרי על הדיווח והאסקלציה אל מול דרג מקבלי ההחלטות במגזר.

<u>דרישות התפקיד:</u>

- אקדמאי בעל תואר ראשון במדעי המחשב או בהנדסת מחשבים, אלקטרוניקה, חשמל ומחשבים, תקשורת. תואר שני יתרון.
- ניסיון מקצועי בתשתיות תקשוב, אבטחת מידע ומערכות בקרה;
- ניסיון בניהול צוות טכני וחדרי מצב NOC/SOC
- יכולת עבודה תחת לחץ ועמידה בלוחות זמנים
- יוזמה אישית; יכולת לימוד ועבודה עצמאית ובצוות;

4.5.1.4. **מנהל\ת אדמיניסטרטיבי\ת**

<u>תיאור התפקיד:</u> אחריות תקשורת מול הגופים (תיאומי פגישות, סיכומים מעקב אחרי משימות), כמו כן יידרש להעלות תכנים, להפיץ חומר טכנולוגי מקצועי ומודיעיני ממקורות שונים, קבלתם, עריכתם והפצתם למגזר.

<u>דרישות התפקיד:</u>

- אקדמאי בעל תואר ראשון ממוסד מוכר עם ניסיון בבנייה ותפעול של אתרים באינטרנט.
- ביצוע קליטה, עדכון, טיוב ובקרת איכות לנתונים בבסיס הנתונים.
- שליפה של נתונים והעברתם לעדכון ולטיוב.
- ביצוע בקרת איכות ובדיקות נתונים.
- קשר עם גורמי תמיכה.
- טיפול והפצה של במשוב, דוחות וסקרים למגזר.

4.5.1.5. **מנהל תשתיות (מקביל לתפקיד בהתאם להוראת תכ"מ 16.2.11 - מקצוע 6.1 -אחראי מערכות מידע רמה ב').**

<u>תיאור התפקיד</u>: אחראי על כל ניהול תשתיות הענן, המערכות והמוצרים של מרכז הTSOC , ניהול הרשאות IDP, ניהול תשתיות התקשרות ואבטחת המידע של המרכז ועוד.

<u>דרישות התפקיד</u>:

- אקדמאי בעל תואר ראשון במדעי המחשב או בהנדסת מחשבים.
- ניסיון של 5 שנים לפחות בניהול מערכות ענן + IT .
- עוסק בתחום מערכות הפעלה מערכות אחסון וגיבויים. בעל הכשרות הרלוונטיות לניהול סביבת בהתאם לאפיון הציע וכ"ו
- ניסיון של 5 שנים במתודולוגיות ניהול פרויקטים
- ניסיון בהפעלת קבלי משנה.
- ידע וניסיון במערכות וירטואליזציה ואחסון נתונים, בתשתיות מיקרוסופט, מוצרי אבטחת מידע (FIREWALL IPS/IDS, ANTIVIRUS FORTINET ועוד)
- ניסיון של 5 שנים לפחות בתחום הגיבויים.

4.5.2. באפשרות הספק להציע אופציה נוספת לתפעול המערכת במבנה ותצורה שונים ממה שמוצע במכרז זה ובלבד שיעמוד בדרישות המכרז לעניין תפעול המערכת. הצעת הספק לתפעול המערכת לא תחייב את המשרד והוא רשאי לקבל אותה, לדחות אותה או לקבל חלקים ממנה.

4.6. **חומרה: תחנות קצה, Storage התקני תקשורת ואבטחת מידע (S)**

- יש לפרט אלו רכיבים נדרשים ע"מ להבטיח שרידות וביצועים בזמינות של: 99.0% שהם חוסר בזמינות של: 365 ימים בשנה, 720 שעות בחודש, 168 שעות בשבוע.
- יש לציין את שם היצרן, דגם ומודל עבור כל ציוד חומרה שנדרש עבור הפתרון.
- יש לפרט את דרישות סביבת הענן עבור כלל המערכות המוצעות והנפחים – בנוסף יש לפרט את הרישוי הדרוש והעלויות לשנה 1 + 3.
- יש לפרט את דרישות החומרה המומלצות עבור תחנות העבודה.
- יש לפרט את התקני התקשורת וה-Firewall המוצע, עדכוני גרסאות ואופן השימוש.
- יש לספק מפרט רכיבים/תוכנות הנדרש ליישום יתירות הרכיבים השונים.

יש להתייחס במענה לנושא גרסאות/עדכונים עתידיים ופרישתם על פני שנה קלנדרית.

<u>הערה</u>: רכיבי חומרה עליהם תפעל המערכת הינם רכוש המשרד והם יפעלו מחצר הלקוח, דהיינו ממרכז ה-TSOC.

4.7. תוכנה: מערכת הפעלה, אפליקציות, DBs, Hypervisor (S)

המציע מתבקש לתאר בפרוטרוט את טכנולוגיות הפיתוח של הפתרון המוצע, תינתן עדיפות למערכות שפותחו ע"פ סטנדרטים עדכניים העומדים בתקנים של גופי תקינה בינלאומיים.

4.7.1. תוכנה (S)

- יש לציין את שם היצרן וגרסת מערכת ההפעלה לכל שרת ו\או תחנת קצה עבור הפתרון.
- יש לציין את שם יצרן וגרסת ה-hypervisor שתותקן עבור הפתרון.
- יש לציין את שם היצרן, שם האפליקציה והגרסה שתותקן עבור הפתרון (עבור כל אפליקציה).
- יש לציין את שם היצרן וגרסת בסיס הנתונים שתותקן עבור הפתרון.
- יש לפרט את רשימת כל תוכנות התשתית הנדרשות עבור המערכת המוצעת, גרסאות של כל רכיב תוכנה ואת סוגי הרישוי (כולל עבור סביבת הבדיקות).
- יש לפרט את כלי הבדיקה הממוחשבים בהם משתמש הספק לצורך בדיקות ביצועים.

במידה והרכישה תתבצע באמצעות המציע, על המציע לרשום את רישיון המוצרים על שמו של הלקוח דהיינו, על שם המשרד.

4.7.2. שדרוגים ועדכוני גרסאות (S)

- יש לפרט את מנגנון עדכוני גרסאות החומרה ברמת התדירות, מערכות הפעלה וה-Embedded, שלבי העדכון בסביבת ה-Testing ובסביבת ה-Production וכ"ו.
- יש לפרט את נוהל עדכון מערכות אבטחת המידע ברמת התדירות, מערכות הפעלה וה-Embedded, שלבי העדכון בסביבת ה-Testing ובסביבת ה-Production וכו'.

- יש לפרט את נוהל עדכון גרסאות התוכנה ברמת תדירות, מערכות הפעלה וה-Embedded, שלבי העדכון בסביבת ה-Testing ובסביבת ה-Production וכו'.

5. מימוש הפרויקט

5.1. **כללי – (I)**

מימוש הפרויקט על כל שלביו כולל אחריות מלאה של הזוכה על כל תחום רלבנטי למחזור החיים של המערכות.

5.2. **דרישות (M)**

המציע נדרש להציג את דרך ניהול הפרויקט ומימושו לרבות הדרישות הבאות:

- ניתוח ואפיון של דרישות הפתרון עבור כלל השלבים.
- בניית גאנט מפורט של אבני דרך ולוחות זמנים בפרויקט.
- ביצוע פיילוט.
- מבדקי מסירה וקבלה.
- הדרכות על כלל המערכות בפרויקט.
- תיעוד כלל בפרויקט.
- ליווי והטמעה.
- תפעול

5.3. **גורמים מעורבים**

5.3.1. **מנהל פרויקט מטעם המשרד (I)**

המשרד ימנה מנהל מטעמו לפרויקט. מנהל הפרויקט יהיה אחראי לאישור תוצרים ואבני דרך, מענה לשאלות, בקשות לשינוי וכד', וכן להגדרת נהלי עבודה לאורך הפרויקט.

5.3.2. **מלווים נוספים מטעם המשרד (I)**

ר' יחידת הסייבר המגזרית ילווה את ה TSOC- ויהווה גורם מקצועי שיהיה אחראי על ההתנהלות של מרכז ה TSOC מול המנהל ה TSOC מטעם המציע לאחר סיום ההקמה.

5.3.3. **מנהל פרויקט מטעם המציע (M)**

מנהל פרויקט מטעם המציע יפעל במשרה מלאה לכל תקופת הפרויקט עד לסיום שלב ההתקנה, ההפעלה בייצור ופעילויות ההטמעה.

5.3.4. **צוות מקצועי מטעם המציע (S)**

המציע יפרט את הצוות המקצועי המועמד לביצוע הפרויקט ובכלל זה את המועמד לניהול הפרויקט מטעמו.

המשרד שומר לעצמו את הרשות לבקש להחליף איש צוות עפ"י שיקוליו וזאת מבלי לפרט או לספק סיבה. בקשה להחליף איש צוות תינתן בהתראה של לפחות חודש ע"מ לתת למציע זמן התארגנות להחלפתו.

5.4. **תכנית עבודה (S)**

המשרד מעוניין להטמיע ולהפעיל את מערכת ה TSOC-בהקדם האפשרי (לאחר חתימה על הסכם התקשרות) בארבעה שלבים עיקריים:

- **שלב א' - אפיון מפורט מרכז ה TSOC** - אפיון מפורט, פיתוח והקמת מרכז ניטור אבטחת סייבר (TSOC).
- **שלב ב' - הקמת מרכז שליטה ובקרה (TSOC) ומערכת שו"ב** - הוכחת יכולת בהפעלת כלל המערך הטכנולוגי למול 4-5 גופים עפ"י הגדרת המשרד, תוך הפעלת סט חוקים בסיסי (כ-30 חוקים שייקבעו ע"י הספק וכ-10 חוקים שיוגדרו ע"י המשרד לפיתוח). השלב יסתיים בבדיקת קבלה שתכלול גם בניית יכולת הצגת תמונת מצב מגזרית , הדרכת צוותים טכניים ויצירת יכולת טכנולוגית וממשק לניתוח אירועים. כמו כן בניית יכולת, כלים ותו"ל להפעלת צוות ה TSOC וצוות ההנחייה המגזרי אשר יוכל במידת הצורך לסייע לג"מים בזמן אמת.
- **שלב ג' - מוכנות להפעלה**– הרחבת הפרישה, היכולות ומבצוע הסביבה לכלל הגופים אשר יוגדרו על ידי המשרד (כ-20 גופים).
- **שלב ד' - הפעלה** - מעבר של המרכז משלב ה POC לשלב מבצעי בו מחוברים למרכז ומנוטרים כלל הגופים שהוגדרו על ידי המשרד והמשך חיבור גופים על פי תוכנית העבודה שתיקבע על ידי המשרד.

הצגת תכנית עבודה שמקצרת את משך הפרויקט (באופן ריאלי) תהווה שיקול בבחירת ההצעה הזוכה.

5.5. **תכנית כללית (S)**

5.5.1. **שלבים/אבני דרך**

על הזוכה להתחיל בביצוע הפרויקט לא יאוחר מ14 ימים לאחר חתימה על הסכם ההתקשרות עמו ולהשלים את יישום הפרויקט לפי לוח-הזמנים הבא:

5.5.1.1. **לוחות הזמנים ואבני דרך בפרויקט:**

5.5.1.1.1. <u>שלב א'</u> - אפיון מפורט מרכז TSOC, על פי דרישות המשרד – עד 1.5 חודש קלנדרי מיום חתימת ההסכם.

5.5.1.1.2. <u>שלב ב'</u> – חלק ב'1 - פיתוח המערכת בהתאם לאפיון המפורט – עד 2 חודשים קלנדריים ממועד אישור האפיון המפורט על ידי המשרד. כולל מבחני קבלה ותיקונים.

5.5.1.1.3. <u>שלב ב' – חלק ב'2</u> – הרצת המערכת בפיילוט שייקבעו על ידי המשרד – עד 1 חודש קלנדרי ממועד סיום מבחני הקבלה ותיקונים. בשלב זה תיבדק עבודה במצבי חרום, קרי: השתלטות מרוחקת מאתר הגיבוי וההתאוששות מאסון.

5.5.1.1.4. <u>שלב ג' – חלק ג'1</u> – הטמעת הג"מים באופן מדורג לפי תיעדוף שייקבע על ידי המשרד – בהתאם למועדים שייקבעו על ידי המשרד – עד 2 חודשים קלנדריים ממועד סיום הפיילוט ואישור המשרד להטמעת המערכת.

5.5.1.1.5. <u>שלב ג' – חלק ג'2</u> – מערכת מבצעית לאחר מבחני קבלה והטמעה. עד 2 שבועות קלנדריים לרבות סיום חיבור כלל הג"מים המוגדרים על ידי המשרד.

5.5.1.1.6. <u>שלב ד' – הפעלה</u>

- לכל שלב מהווה אבן דרך בפרויקט ודורש אישור כתוב של הממונה מטעם המשרד לצורך התקדמות לשלב הבא.

- השלמת אבן דרך ע"י המציע ואישורה הכתוב ע"י הממונה מטעם המשרד מהווים אישור לתשלום החלק היחסי של העלות בהתאם לאחוז ההתקדמות בפרויקט.

- אישור מסירה של המערכת יתבצע בקרות מוקדם מבין הבאים: (1) סיום מוצלח של מבחני הקבלה; או (2) תחילת הפעלת המערכת בייצור ע"י המשרד;

5.5.1.2. **לוחות הזמנים (S)**

על המציע לעמוד בלוח זמנים לפיתוח המערכות\הסביבות והטמעת ה-TSOC על כל שלביו , לוח הזמנים יהיה בהלימה

עם לוח הזמנים שקבע המשרד והוא לא יכול לחרוג ממנו מראש.

עם חתימת החוזה ייבנה לוח זמנים מפורט של כל מרכיבי המערכת בחלוקה לפי שלבים ואבני דרך. לוח הזמנים יאושר ע"י שני הצדדים ויהווה בסיס למעקב אחר ההתקדמות ועמידה ביעדים.

דיונים לצורך מעקב אחר התקדמות יתקיימו באופן שוטף ובתדירות שתיקבע על ידי המשרד. עבור פעילויות בפיגור יהא על מנהל הפרויקט מטעם הזוכה להציג ולבצע פעולות מתקנות לשם סגירת הפערים.

5.6. **תיעוד (S)**

<u>מסמכים שיימסרו למשרד:</u>

- אפיון מפורט למערכת ולממשקים - בתום אבן דרך שלב א'.
- תכנית בדיקות - בתום אבן דרך חלק ב' – שלב ב'.
- מסמכים שיימסרו במהלך ההטמעה ובסיום הפרויקט - במסגרת אבן דרך חלק ג' שלב ב':
  - מסמך תכולת גרסה.
  - תיק תחזוקה הכולל:

✓ תיאור קונפיגורציה ופרמטרים ספציפיים וסופיים של המערכת לאחר ה- FINE TUNING (כיול) המותאם לכלל המערכת.

✓ קונפיגורציה, פרמטרים וגרסאות של: מערכת הפעלה, שרתים ותחנות קצה, מנוע ה-WEB (במידת הצורך) או כל טכנולוגיה שהיא.

✓ תיאור בכתב של התהליך וכל הפעולות הנדרשות לאתחול המערכת מ"אפס" למקרה הצורך ו/או התאוששות מאסון, כולל שרת, IIS, DB, וכו'.

  - מדריך למשתמש.
  - רישיונות ורישוי תוכנות כולל צד-שלישי

תוצרי התיעוד למעט חוזים ותיעוד של יצרני התוכנה יימסרו למשרד עד למועד סיום הפרויקט (שלב ב', סיום התקנה והטמעה).

התיעוד יימסר ע"ג מדיה מגנטית בת עדכון ובנוסף בעותקים מודפסים.

תיעוד המערכת מהווה חלק מאבן הדרך בהשלמת הפרויקט.

5.7. אחריות (I)

לאורך כל תקופת ההתקשרות וההפעלה האחריות לתחזוקה, לרישוי ולטיפול בתקלות בכלל המערכות הינה על המציע.

5.7.1. מבחני קבלה

המשרד יבצע למערכת בדיקות קבלה. במידה ויימצאו ליקויים או אי-דיוקים, המשרד יעביר את הערותיו לזוכה לצורך ביצוע התיקונים הנדרשים, וייקבע מועד מסירה חדש. התהליך יחזור על עצמו עד לקבלת מערכת לפי קריטריונים שהוגדרו בעת אפיון המפורט. המשרד שומר לעצמו את הזכות לבצע מבחני קבלה בכוחותיו הוא ו/או באמצעות קבלן חיצוני, בטרם יאשר את קבלת המערכת. מוסכם, כי במידה ולא אישר המשרד את מבחני הקבלה כאמור בסעיף זה ולא הוגשה כל הסתייגות על ידי המשרד ו/או רשימת ליקויים במועדים שנקבעו במסמך האפיון ,או במועד מאוחר יותר עליו הודיע המשרד בהודעה שניתנה לפני המועד שנקבע במסמך האפיון ,ייחשב הדבר כאישור מבחני הקבלה על ידי המשרד לכל דבר ועניין החל מהמועד המוסכם לאישור מבחני הקבלה או מתום 14 ימים ממועד אבן דרך/מערכת לאישור המשרד, לפי המאוחר.

5.7.2. זמינות ושרידות (I)

המערכת שתסופק תשרת את המשרד 7 ימים, בשבוע 24 שעות ביממה. על המציע לפרט את הפעולות הדרושות לזמינות ועמידה ב- SLA שנקבע למערכת על כלל מרכיביה ומכלולה 99.0% תוך התייחסות למצבים הבאים:

- משך זמן התאוששות מרגע הנפילה (RTO, RPO).
- התייחסות לפרק הזמן בין נפילה ועד לעליה מחדש של המערכת (MTTR).
- התייחסות לפרק הזמן שבין נפילה ונפילה (MTBR).
- משך זמן השבתה עבור עדכונים תוכנה.
- משך הזמן הנדרש בהשבתות לצורך שדרוג המערכת.

5.7.3. גיבויים (S)

גיבויי מערכת באחריות הספק ובאמצעות המערכות והתשתיות שאופיינו, הוטמעו ונבדקו בפרויקט ועומדות לרשותו. המציע אחראי

להגדיר תכנית גיבויים שתכלול פירוט הרכיבים אותם יש לגבות וכן את יישומה ושמירה על אבטחת המידע בגיבויים.

5.7.4. **שחזור והתאוששות מנפילה (S)**

אחת לפרק זמן שיקבע עם הספק (לא יעלה על שנה) תבוצענה פעולות לבדיקת תקינות, מהימנות וחיות של הגיבויים:

- יבוצע שחזור מדגמי לנתונים שנמצאים באתר הגיבוי כפי שיאושר בארכיטקטורה שתסוכם.
- תבוצע בדיקת שחזור מלאה לנתונים שגובו באתר הגיבוי וההתאוששות מאסון.
- תבוצע סימולציה למצב של התאוששות מאסון של המערכות.

6. אבני דרך לתשלום:

אבני הדרך לתשלום התמורה לזוכה יהיו כמפורט להלן:

6.1. <u>לוחות הזמנים ואבני דרך בפרויקט:</u>

תיאור השלב	**לוחות זמנים**	אבן דרך לתשלום **(%מהמחיר לשלב <u>הקמת המערכת</u>)**
שלב א'- אפיון מפורט מרכז TSOC, על פי דרישות המשרד	עד 1.5 חודשים קלנדריים מיום חתימת ההסכם	15%
שלב ב' - חלק ב'1 - פיתוח המערכת בהתאם לאפיון המפורט וביצוע מבצעי קבלה	עד 2 חודשים קלנדריים ממועד אישור האפיון המפורט על ידי המשרד	20%
שלב ב' – חלק ב'2 – הרצת המערכת בפיילוט שייקבעו על ידי המשרד	עד 1 חודש קלנדרי ממועד סיום מבחני הקבלה ותיקונים. בשלב זה תיבדק עבודה במצבי חרום, קרי: השתלטות מרוחקת מאתר הגיבוי וההתאוששות מאסון.	15%
שלב ג' - חלק ג'1– המשך פיתוח והטמעת המערכת באופן מדורג לפי תיעדוף שייקבע על ידי המשרד – בהתאם למועדים שייקבעו על ידי המשרד	עד 2 חודשים קלנדריים ממועד סיום הפיילוט ואישור המשרד להטמעת המערכת.	30%
שלב ג' – חלק ג'2 מערכת מבצעית לאחר מבחני קבלה והטמעה.	עד 2 שבועות קלנדריים ממועד סיום חיבור כלל הג"מים המוגדרים על ידי המשרד	20%
שלב ד' - הפעלה	ישולם באופן חודשי עפ"י מנגנון החישוב המופיע בסעיף 5.2	

פרק ד' – הסכם התקשרות

הסכם התקשרות

ב י ן

משרד התחבורה

(להלן: "**המזמין**")

<u>מצד אחד</u>

ל ב י ן

_____

מכתובת _____

(להלן: "**הספק**")

<u>מצד שני</u>

הואיל והמזמין פרסם את מכרז 11/2026 לאפיון, הקמה והתפעול של מרכז ניטור ותגובה סייבר במגזר התחבורה (TSOC) (להלן: "**המכרז**"), לקבלת המוצרים והשירותים המפורטים ב**פרק ג** למכרז ("**המוצרים והשירותים**");

והואיל והספק הגיש הצעה למכרז, כדי לספק את המוצרים והשירותים המבוקשים בהתאם לאמור במכרז, בהצעתו ובהסכם זה (להלן: "**ההסכם**");

והואיל ובכפוף לחתימתו על ההסכם וקיום הדרישות המפורטות במכרז, ועדת המכרזים של המזמין בחרה בספק כזוכה במכרז;

לפיכך הוצהר, הותנה והוסכם בין הצדדים כדלקמן:

1. כללי

1.1. להסכם זה מצורפים הנספחים המפורטים להלן:

1.1.1. **נספח א'** – פירוט השירותים (פרק ג' למסמכי המכרז);

1.1.2. **נספח ב'** – חוברת ההצעה של הספק במכרז;

1.1.3. **נספח ג'** – ערבות ביצוע;

1.1.4. **נספח ד'** – נספח סודיות והיעדר ניגוד עניינים;

1.1.5. **נספח ה'** – כללי הצמדה של התמורה;

1.1.6. **נספח ו1'** – נספח סייבר ואבטחת מידע;

1.1.7. **נספח ו2'** – נספח סייבר ואבטחת מידע ייעודי.

1.2. בנוסף מסמכי המכרז והבהרות למכרז שפורסמו באתר מינהל הרכש הממשלתי (בהתאם לנוסח המעודכן ביותר המופיע שם), ייחשבו גם הם כמצורפים להסכם זה.

1.3. המבוא והנספחים להסכם מהווים חלק בלתי נפרד ממנו.

בהסכם תהיה למונחים המשמעות המופיעה במכרז. פרשנות ההסכם על נספחיו תיעשה באופן המקיים את דרישות המכרז המפורשות והמשתמעות ואת תכלית המכרז של אספקת המוצרים והשירותים למזמין באופן מיטבי .

2. תקופת ההתקשרות

תקופת ההתקשרות תארך 24 חודשים ממועד החתימה על הסכם זה **("תקופת ההתקשרות")**, כאשר למזמין הזכות להאריך את תקופת ההתקשרות בתקופות נוספות, ועד ל - 48 חודשים נוספים (6 שנים סה"כ), על פי שיקול דעתו הבלעדי.

<u>תקופת התארגנות</u> – תקופה של עד שבועיים הראשונים מתוך תקופת ההתקשרות תהווה תקופת התארגנות. בתקופה זו יבצע הספק את כל הפעולות הנדרשות ממנו כהיערכות לשם התחלת מתן השירותים. המזמין רשאי להאריך את משך תקופת ההתארגנות בהתאם לשיקול דעתו הבלעדי.

2.1. <u>תקופת מעבר</u> – תקופה של 45 הימים האחרונים של ההתקשרות, תהווה תקופת מעבר. בתקופה זו יהיה רשאי המזמין להתקשר עם ספקים אחרים בנושא ההתקשרות והיקף השירותים אשר יירכשו מהספק בתקופה זו יפחת לפי צרכי המזמין. כמו כן, בתקופה זו הספק ישתף פעולה עם המזמין ועם הספק החדש שייבחר על ידי המזמין בנושא ההתקשרות, לביצוע כל הפעולות הנדרשות לשם העברת ביצוע נושא ההתקשרות לספק החדש.

כל שינוי בתקופת ההתקשרות וכן מימוש הזכות להאריך את ההתקשרות, יכנס לתוקפו רק עם חתימה של מורשיי החתימה מטעם המזמין.

3. התחייבויות והצהרות הספק

3.1. הספק מצהיר ומתחייב כי -

3.1.1. אין מניעה לפי כל דין להתקשרותו בהסכם.

3.1.2. הוא עומד בכל דרישות הדין הרלוונטיות לאספקת המוצרים והשירותים בהתאם להסכם.

3.1.3. ברשותו הניסיון, המיומנות, הידע, הכלים, המלאי וכוח האדם הדרושים למילוי חובותיו בהתאם לתנאי ההתקשרות.

3.1.4. הוא יספק את הנדרש ממנו על פי דרישות ההתקשרות, לשביעות רצון המזמין.

3.1.5. הוא ישתף פעולה עם המזמין וכל נציג מטעמו בכל הקשור למילוי התחייבויותיו על פי הסכם זה, בכלל זה הוא ישתף פעולה באופן מלא עם הוראות קב"ט המזמין.

4. סודיות

4.1. הספק מתחייב כי הוא ומי מטעמו ישמרו את המידע שהתקבל אצלם במהלך ביצוע חובותיהם על פי ההסכם והמכרז בסודיות מוחלטת, במהלך תקופת ההתקשרות ולאחריה, ולא יעשו בו כל שימוש למעט לצורך ביצוע חובותיהם בהתאם למכרז ולהסכם.

4.2. לעניין התחייבות זו לסודיות מובהר כי הגדרת "מידע" או "מידע סודי" לא תכלול:

4.2.1. מידע שהוא נחלת הכלל או שיהפוך לנחלת הכלל שלא עקב הפרת התחייבות זו.

4.2.2. מידע שהיה בידי הספק טרם החתימה על ההסכם.

4.2.3. אם הספק או מי מטעמו יפנו בבקשה מתאימה להחרגתו של סוג מידע מסוים מתחולת המידע הסודי, או לחשיפתו בפני גורם כלשהו, המזמין ידון בבקשה ויהיה רשאי לקבלה, בהתאם לשיקול דעתו הבלעדי בתנאי שאין בחשיפת המידע חשש לפגיעה כלשהי באינטרסים של המזמין.

4.3. הספק אחראי לכך כי בעלי תפקידים אצלו וקבלני משנה שלו, אשר במסגרת עבודתם נחשפים למידע של המזמין, ישמרו על המידע אליו הם נחשפו בסודיות, בהתאם לחובותיו על פי הסכם זה.

5. אבטחת מידע והגנות סייבר

5.1. הספק יהיה האחראי הבלעדי על אבטחת המידע של המזמין המגיע לרשותו או נצבר אצלו בקשר עם ביצוע ההסכם באמצעי אבטחה נאותים בהתאם למפורט בנספח ו1' – נספח סייבר ואבטחת מידע ובהתאם למפורט בנספח ו2- נספח סייבר ואבטחת מידע ייעודי. הספק יציג למזמין, אם יידרש, את האמצעים בהם הוא נוקט לשם אבטחת המידע, ויפעל בהתאם לדרישות מאת המזמין לתיקון כל ליקוי או פרצה באבטחת המידע והגנות הסייבר.

6. ניגוד עניינים בביצוע ההסכם

6.1. הספק מתחייב כי אין בביצוע ההסכם כדי ליצור ניגוד עניינים כלשהו, בין במישרין ובין בעקיפין, בינו לבין המזמין.

6.2. בכל מקרה שיווצר חשש כלשהו לניגוד עניינים בין הספק לבין המזמין יודיע הספק על כך למזמין, ללא כל שיהוי ויפעל באופן מידי להסרת ניגוד העניינים. בנוסף, במקרה כאמור, יודיע המזמין לספק אודות אמצעים נוספים או מיוחדים הנדרשים ממנו לצורך הסרת ניגוד העניינים, והספק יבצע את הנדרש ממנו בהקדם.

6.3. הספק מתחייב להחתים כל אחד מעובדיו ומי מטעמו שיועסקו על ידו לצורך ביצוע ההסכם על הצהרת הסודיות והיעדר ניגוד עניינים בנוסח המופיע כ**נספח ד'** להסכם זה.

7. קניין רוחני וזכויות יוצרים

7.1. הספק הוא בעל הזכויות הנדרשות לצורך אספקת השירותים והשימוש בהם על-ידי המזמין ("**זכויות הקניין הרוחני**"). במקרה שהספק אינו בעל מלוא זכויות הקניין הרוחני, הוא מצהיר כי בעלי זכויות הקניין הרוחני נתנו בידיו את כל האישורים, הרשאות השימוש והרישיונות הדרושים לפי כל דין לצורך אספקת השירותים והשימוש בהם על-ידי המזמין, בהתאם לתנאי הסכם זה.

7.2. בעת ביצוע ההתקשרות, הספק לא יעשה שימוש בתוכנות מחשוב, תמונות, מסמכים וכיוצא באלה, שהוא אינו מורשה על-פי דין לעשות בהם שימוש.

7.3. תוצר שהוכן על ידי הספק במהלך תקופת ההתקשרות עבור המזמין ובכלל זאת, נתונים, מצגות, מסמכים, סיכומי פגישות, תמונות, תכנים וכיוצא בזה ("**תוצרי העבודה**"), הוא קניינו הבלעדי של המזמין והוא יוכל לעשות בו כל שימוש שירצה בעתיד, לרבות פרסום פומבי. הספק לא יהיה רשאי למכור, להעביר, להמחות, לפרסם, להשכיר, לרשום, או לעשות שימוש כלשהו בתוצרי העבודה, ללא אישור המזמין בכתב ומראש.

תוצרי העבודה לא יכללו תהליכי עבודה ומערכות ייעודיות של הספק, אשר לא הוכנו עבור המזמין במסגרת ביצוע ההסכם.

7.4. למען הסר ספק, תוצרי העבודה יהיו רכוש המזמין גם אם מתן השירותים ע"י הספק הופסק תוך כדי תקופת ההתקשרות.

7.5. **הפרת קניין רוחני**

7.5.1. נקבע במסגרת פסק דין חלוט של ערכאה מוסמכת כי שירות שהעמיד ספק לרשות המזמין מפר זכות קניין רוחני של צד שלישי כלשהו, הספק יפעל בהתאם למפורט להלן:

7.5.1.1. הספק יודיע על כך למזמין בהקדם האפשרי.

7.5.1.2. הספק יחדל מאספקת השירות המפר.

7.5.1.3. הספק ייעשה כל מאמץ סביר על מנת להמשיך לספק את השירות באופן שאינו פוגע בקניין רוחני של צד שלישי כלשהו, וזאת תוך עמידה בחובותיו לפי ההסכם, ומבלי לפגוע ברמת השירות.

8. קבלני משנה

8.1. בכפוף לאמור במסמכי ההתקשרות, הספק יהיה רשאי להפעיל קבלני משנה עבור:

8.1.1. צוות התערבות (IR) – נדרש להיות בשיוך אחת מחברות המשתתפות בפרויקט "Mirror" בהובלת מערך הסייבר.

8.1.2. דסק מודיעין סייבר

לא יותר שימוש בקבלני משנה במסגרת ביצוע ההתקשרות, למעט האמור בסעיף זה.

8.2. מבלי לגרוע מהאמור, האחריות הכוללת לביצוע ההתקשרות ולעמידה בכל תנאיה תהיה של הספק ושלו בלבד.

בכל מקרה שהספק יעסיק קבלן משנה ייעודי לצורך ביצוע הוראות ההסכם ולצורך זה בלבד, המזמין יהיה רשאי לדרוש מהספק להחליף קבלן משנה זה אם הוא סבור כי הוא אינו מבצע את חובותיו כנדרש.

9. יחסים בין הצדדים

9.1. מוצהר ומוסכם בזה בין הצדדים כי:

9.1.1. היחסים ביניהם לפי ההסכם אינם יחסי עובד ומעביד והמזמין אינו המעסיק של עובדי וקבלני המשנה של הספק.

9.1.2. הספק בלבד יהיה אחראי לכל תשלום, לשיפוי בגין נזק, פיצויים או כל תשלום אחר המגיע ממנו על פי כל דין לאנשים המועסקים על ידו בין באופן ישיר בין כקבלני שירות, או לכל אדם אחר.

9.1.3. המזמין לא ישלם כל תשלום לביטוח לאומי ויתר הזכויות הסוציאליות בקשר לאנשים המועסקים על ידי הספק.

9.1.4. אם למרות האמור לעיל, ערכאה שיפוטית או מינהלית מצאה כי המזמין נושא באחריות ישירה כלפי הספק, עובדיו או קבלני משנה שלו, כאילו הוא מעסיקם, ישפה הספק את המזמין עבור כל תשלום בו הוא חויב וחורג מהתמורה המגיע לו לפי הסכם זה. בכלל זה יישא הספק בתשלומי הוצאות משפט ושכר טרחת עורך דין בהם נשא המזמין.

9.1.5. במקרה של הגשת תביעה כאמור בסעיף זה, יודיע המזמין לספק על קיומה של התביעה, ויאפשר לספק להתגונן.

10. תמורה

10.1. התמורה לספק תשולם בהתאם למפורט בהצעת המחיר, המצורפת כ**נספח ב'** להסכם.

10.2. התשלום החודשי עבור שירותי התפעול (שלב ד') יחושב על בסיס השירותים שסופקו ואושרו בפועל, בשילוב היקף הגופים המנוטרים, כמפורט להלן:-

10.2.1. **ביצוע בפועל:** החישוב יתבסס על "פירוט עלות הפעלה חודשי" (טבלה 2 בנספח המחיר). מובהר כי לא תשולם תמורה עבור מרכיב (כ"א, רישוי, מערכות או תשתיות) אשר לא הועמד לרשות המזמין או לא תופעל כנדרש במהלך חודש ההפעלה או חלקו.

10.2.2. **התאמה לכמות הגופים המנוטרים:** התמורה החודשית המאושרת (בהתאם לסעיף 10.2.1 לעיל) תוכפל באחוז התשלום הנגזר מכמות הגופים המנוטרים בפועל באותו חודש, לפי המדרגות הבאות:

עלות הפעלת המרכז בקיבולת גופים בהתאם	עד 20 גופים (כולל) – 80% מחודש הפעלה
	מעל 20 ועד 30 גופים (כולל)- 85% מחודש הפעלה
	מעל 30 ועד 40 גופים (כולל)- 90% מחודש הפעלה
	מעל 40 ועד 50 גופים (כולל)- 100% מחודש הפעלה

10.3. תשלום התמורה יעשה לפי ביצוע בפועל ובכפוף לתנאי ההתקשרות.

10.4. **הצמדה של התמורה -**

10.4.1. התמורה תהיה צמודה למדד המחירים לצרכן.

10.4.2. ההצמדה תתבצע בהתאם לכללים המפורטים ב**נספח ה'** להסכם.

10.5. **סופיות התמורה:**

10.5.1. התמורה לספק תהיה סופית, ולא ישולם לספק סכום נוסף כלשהו בגין ביצוע הנדרש ממנו לפי הסכם זה, בכלל זה לא ישולם לספק בגין החזר הוצאות, נסיעות, תשלום עבור קבלני משנה תשלומים לצדדי ג' וכדו', אלא אם צוין אחרת במפורש במסמכי ההתקשרות.

10.5.2. בכל מקרה שבו יחולו שינויים בהוראות הדין באופן המשפיע על ביצוע ההסכם, הספק יישא בעלויות של שינויים אלו, למעט אם נכתב במפורש אחרת במסמכי ההתקשרות.

10.6. **אבני דרך לתשלום**

10.6.1. התמורה תשולם לספק בהתאם לאבני הדרך כמפורט להלן. התשלום בגין כל אבן דרך יעשה אך ורק לאחר השלמת אבן הדרך במלואה, לשביעות רצון המזמין. לא יהיה תשלום על ביצוע חלקי או יחסי של אבן דרך.

תיאור השלב	**לוחות זמנים**	אבן דרך לתשלום **(% מהמחיר לשלב הקמת המערכת)**
שלב א'- אפיון מפורט מרכז TSOC, על פי דרישות המשרד	עד 1.5 חודשים קלנדריים מיום חתימת ההסכם	15%
שלב ב' – חלק ב'1 - פיתוח המערכת בהתאם לאפיון המפורט וביצוע מבצעי קבלה	עד 1.5 חודשים קלנדרי ים ממועד אישור האפיון המפורט על ידי המשרד	20%

שלב ב׳ - חלק ב׳2 – הרצת המערכת בפיילוט שייקבעו על ידי המשרד	עד 1 חודש קלנדרי ממועד סיום מבחני הקבלה ותיקונים. בשלב זה תיבדק עבודה במצבי חרום, קרי: השתלטות מרוחקת מאתר הגיבוי וההתאוששות מאסון.	15%
שלב ג׳ – חלק ג׳1 – הטמעת המערכת באופן מדורג לפי תיעדוף שייקבע על ידי המשרד – בהתאם למועדים שייקבעו על ידי המשרד	עד 2 חודשים קלנדריים ממועד סיום הפיילוט ואישור המשרד להטמעת המערכת.	30%
שלב ג - חלק ג׳2 - מערכת מבצעית לאחר מבחני קבלה והטמעה.	עד 2 שבועות קלנדריים ממועד סיום חיבור כלל הג״מים המוגדרים על ידי המשרד	20%
שלב ד׳ - הפעלה	יישולם באופן חודשי	

11. כללי תשלום

11.1. כללי התשלום המפורטים להלן כפופים להוראות החשב הכללי במשרד האוצר כפי שמתפרסמים מעת לעת.

11.2. לצורך וכתנאי לקבלת תשלומים, הספק ידאג להמציא למזמין צילום תעודת עוסק מורשה על פי חוק מס ערך מוסף, התשל״ו-1975, בתוקף לשנת הכספים בה מתבקש התשלום, אישור מפקיד מורשה כמשמעותו בחוק עסקאות גופים ציבוריים, בתוקף לאותה שנת כספים, כי הוא מנהל או פטור מלנהל את פנקסי החשבונות והרשומות שעליו לנהלם על פי פקודת מס הכנסה [נוסח חדש] ועל פי החוק וחשבון המפרט את התשלומים המגיעים לו בהתאם להסכם (**״חשבון״**). את החשבון על הספק להגיש בהתאם להנחיות המזמין, וזאת כתנאי לאישור החשבון ולהעברת התשלום לספק.

11.3. החשבון יכלול את הפרטים והמסמכים הבאים:

11.3.1. שם הספק וכתובתו, מספר מזהה של הספק, תאריך החשבון, מספר התחייבות או הזמנה, תיאור שירות או עבודה (וכן יחידת מידה, כמות, מחיר יחידה, אם קיים), ערך כולל לפני מס ערך מוסף, סכום מס ערך מוסף בגין החשבונית (מתייחס לעוסק מורשה בלבד), סך הסכום לתשלום – בספרות ובמילים, חתימת הספק או חתימה דיגיטלית וכן קיום הכיתוב ״מסמך ממוחשב״.

11.4. במקרה שבו יחול שינוי בגובה המע״מ תעודכן בהתאם התמורה לה זכאי הספק.

11.5. במקרה בו יהיו שינויים שאינם בגובה המע״מ במסים או בהיטלים, על מחיר השירותים או הטובין, לא יהיה בשינויים אלה כדי להשפיע על גובה התמורה, אלא בהתאם ובכפוף לקבלת אישור המזמין מראש ובכתב, ולפי שיקול דעתו הבלעדי.

11.6. הספק יידרש להגיש דיווחים וחשבוניות באמצעות פורטל הספקים הממשלתי, מערכת ממוחשבת של הממשלה המאפשרת בין היתר הגשת חשבוניות באופן מקוון.

11.7. המזמין יבדוק ויאשר כל חשבון שיוגש לתשלום על ידי הספק, בהתאם למפורט לעיל ולהנחיות החשב הכללי.

11.8. מועד התשלום עבור חשבון שאושר על ידי המזמין, יהיה לא יאוחר מ- 45 ימים מהמועד שבו הומצא החשבון למזמין, ובמקרים חריגים לא יאוחר מ- 30 ימים מתום אותו החודש שבמהלכו הומצא החשבון למזמין.

12. ערבות ביצוע

12.1. כבטחון למילוי ההתחייבויות של הספק על-פי ההסכם ימסור הספק למזמין ערבות אוטונומית בלתי מותנית, בהיקף של 200,000₪.

12.2. ערבות הביצוע תהיה ערבות דיגיטלית בהתאם לתקן הערבויות הדיגיטליות אשר פורסם על יד החשב הכללי, ואשר הונפקה על ידי גוף אשר הוסמך על ידי החשב הכללי להנפקת ערבות דיגיטלית בהתאם לתקן. במקרה כאמור תהיה הערבות בהתאם לנוסח המפורט כנספח ג להסכם, ותנוהל בהתאם לתקן הערבויות הדיגיטליות ולהוראת תכ"ם 7.3.7 ערבויות דיגיטליות.

12.3. הערבות תונפק על ידי גוף המוסמך להנפיק ערבויות בהתאם להוראות המפורטות ב**הוראת תכ"ם 7.3.3 "ערבויות"**.

12.4. גוף סטטוטורי, חברה ממשלתית, חברת בת ממשלתית ומוסד להשכלה גבוהה שהמדינה משתתפת בתקציבו רשאים להגיש הוראת קיזוז במקום ערבות הגשה בהתאם לנוסח המפורט בהוראת תכ"ם 7.3.3 "ערבויות".

12.5. תוקף הערבות יהיה 90 יום לאחר תום תקופת ההתקשרות. אם המזמין יממש את האופציה להארכת תקופת ההתקשרות, יאריך הספק את תוקף הערבות בהתאמה עד ל-90 יום לאחר תום תקופת ההתקשרות.

12.6. המזמין רשאי לדרוש להאריך את תוקף הערבות בעוד שלושה חודשים לאחר תום תקופת הערבות, במקרה בו יהיה הדבר נדרש על מנת להבטיח סיום אספקת השירותים או אחריות או לשם הבטחת עמידת הספק בהתחייבויותיו לפי ההסכם. אם הספק לא יאריך את תוקף הערבות בהתאם להוראות ההסכם, רשאי המזמין לחלט את הערבות, בהתאם לשיקול דעתו הבלעדי.

12.7. במהלך תקופת ההתקשרות רשאי המזמין, לפי שיקול דעתו הבלעדי, להפחית את סכום ערבות הביצוע, לסכום נמוך יותר, כפי שיקבע על ידו.

12.8. לאחר תום התוקף של הערבות, במקרה שהיא לא חולטה, יחזיר המזמין את הערבות לספק.

13. אחריות בנזיקין וחובת שיפוי

13.1. הספק יישא באחריות, לפי כל דין, בגין אובדן או נזק מכל סוג שהוא, שייגרם למזמין, לעובדיו וכל מי מטעמו וכן לכל גוף, אדם או צדדים שלישיים כלשהם, עקב מעשה או מחדל של הספק, עובדיו, שלוחיו, קבלני משנה שלו או כל מי שבא מכוחו או מטעמו, במסגרת ביצוע הסכם זה. הספק מתחייב לדווח למזמין על כל נזק או אובדן כאמור, באופן מידי.

13.2. המזמין, הבאים מכוחו או המועסקים על ידו לא יישאו באחריות ולא יישאו בשום תשלום, הוצאה, אובדן או נזק, בגין נזק מכל סוג שהוא שייגרם לספק, לבאים מכוחו או למועסקים על ידו . האמור לא יחול ביחס לנזק שנגרם בזדון ושהאחריות בגינו מוטלת על המזמין לפי דין.

13.3. הספק יהיה אחראי לתקן כל נזק או אובדן, אם יגרמו עקב ביצוע ההתקשרות ע"י הספק או מי מטעמו, ולהשיב את המצב לקדמותו- במועד הקרוב ביותר לאחר התרחשות הנזק או האובדן. אין באמור, כדי לגרוע מזכות המזמין לתקן את הנזק או האובדן בעצמו ולחייב את הספק בתשלום הוצאותיו. ההחלטה על אופן ביצוע התיקון, תהיה נתונה לשיקול דעתו הבלעדי של המזמין.

13.4. לא יהיה בסיומו של הסכם זה כדי לגרוע מאחריות הספק לגבי נזקים שעילת התביעה בגינם נובעת מהסכם זה או מאספקת השירותים על פיו או קשורה אליהם.

13.5. הספק מתחייב לשפות את המזמין באופן מלא, במקרה שיחויב המזמין בפסק דין חלוט של ערכאה שיפוטית מוסמכת, ולשלם כל סכום בגין חיוב שעל פי הסכם זה חב בו הספק, ובתוספת כל הוצאותיו של המזמין, לרבות הוצאות משפטיות ושכר טרחת עורך דין שיהיו לו בקשר לתביעה בגין האמור, וכן בתוספת הפרשי הצמדה וריבית על פי דין. חובת השיפוי כאמור תחול בין אם השיפוי נובע מתביעתו של עובד של הספק או מי מטעמו של הספק (לרבות קבלני משנה) או עובד של המזמין או צד שלישי או של מבטח או מכל מקור אחר. הסכומים כאמור ישולמו למזמין מיד עם הגשת דרישתו בכתב ובה פירוט ההוצאות שנגרמו לו כאמור.

13.6. טענות צד שלישי

13.6.1. הועלתה ע"י צד שלישי, טענה שעילתה נובעת או קשורה להתקשרות זו לרבות, הפרת זכויות קניין הרוחני או נזקים שנגרמו לצד שלישי כלשהו (להלן: "**טענת הפרה**"), יפעלו הצדדים בהתאם למפורט להלן:

13.6.2. הצדדים יעדכנו אחד את השני בדבר הטענה ועילתה,בהקדם האפשרי על מנת לאפשר לכל צד להתגונן כלפי הטענה.

13.6.3. במקרה בו הוגשה תביעה בטענה כאמור, רשאי המזמין לדרוש מהספק להיכנס בנעלי המזמין לצורך ניהול ההליך.

13.7. תקרת אחריות –

13.7.1. גבול אחריות הספק לפיצוי או שיפוי המזמין עבור כל אירוע נזק לא יעלה על גובה הנזק שנגרם או השיפוי שנדרש **ועד 1 פעמים היקף ההתקשרות,** לפי הסכום הנמוך מביניהם, ובתוספת כל הוצאותיו של המזמין, לרבות הוצאות משפטיות ושכר טרחת עורך דין שיהיו לו בקשר לתביעה בגין האמור, וכן בתוספת הפרשי הצמדה וריבית על פי דין.
הסכומים כאמור ישולמו למזמין מיד עם הגשת דרישתו בכתב ובה פירוט ההוצאות שנגרמו לו כאמור.
הגבלת האחריות האמורה לא תחול על נזק שייגרם על ידי מעשה או מחדל שנעשו בזדון על ידי הספק, עובדיו או קבלני המשנה ומי מטעמו.

14. ביטוח

א. **הספק מתחייב לרכוש ולקיים את כל הביטוחים המפורטים בזה, לטובתו ולטובת מדינת ישראל – משרד התחבורה והבטיחות בדרכים, כשהם כוללים את כל הכיסויים והתנאים הנדרשים כאשר גבולות האחריות לא יפחתו מהמצוין להלן:**

14.1. ביטוח חבות מעבידים

14.1.1. הספק יבטח את אחריותו החוקית על פי פקודת הנזיקין (נוסח חדש) ו/או חוק האחריות למוצרים פגומים תש"ם -1980 כלפי עובדיו בביטוח חבות מעבידים בכל תחומי מדינת ישראל והשטחים המוחזקים.

14.1.2. גבול האחריות לא יפחת מסך- 20,000,000 ₪ לעובד, למקרה ולתקופת הביטוח.

14.1.3. הביטוח יורחב לכסות את חבותו של המבוטח כלפי קבלנים, קבלני משנה ועובדיהם היה ויחשב כמעבידם.

14.1.4. הביטוח יורחב לשפות את מדינת ישראל - משרד התחבורה והבטיחות בדרכים, היה ונטען לעניין קרות תאונת עבודה/מחלת מקצוע כלשהי כי הם נושאים בחבות מעביד כלשהם כלפי מי מעובדי הספק, קבלנים, קבלני משנה ועובדיהם שבשירותו.

14.2. ביטוח אחריות כלפי צד שלישי

14.2.1. הספק יבטח את אחריותו החוקית על פי דיני מדינת ישראל בביטוח אחריות כלפי צד שלישי גוף ורכוש (כולל נזקי גרר), בכל תחומי מדינת ישראל והשטחים המוחזקים.

14.2.2. גבול האחריות לא יפחת מסך- 4,000,000 ₪ למקרה ולתקופת הביטוח.

14.2.3. בפוליסה ייכלל סעיף אחריות צולבת - Cross Liability.

14.2.4. הביטוח יורחב לכסות את חבותו של המבוטח כלפי צד שלישי בגין פעילות של קבלנים, קבלני משנה ועובדיהם.

14.2.5. הביטוח יורחב לשפות את מדינת ישראל - משרד התחבורה והבטיחות בדרכים, ככל שייחשבו אחראים למעשי ו/או מחדלי הספק וכל הפועלים מטעמו.

14.3. ביטוח משולב לאחריות מקצועית וחבות המוצר

COMBINED PRODUCTS LIABILITY AND PROFESSIONAL INDEMNITY POLICY FOR THE SOFTWARE AND HARDWARE INDUSTRY.

או

ELECTRONIC PRODUCTS AND SERVICES ERRORS OR OMISSONS AND PRODUCTS LIABILITY INSURANCE

או

נוסח אחר לביטוח משולב לאחריות מקצועית וחבות המוצר לענף הייטק/תחום מחשוב כדלהלן: _____ **(בכפוף לבחינתה ולשיקולה של ענבל).**

14.3.1. הספק יבטח את אחריותו בגין הקמת מרכז ניטור אבטחת סייבר במגזר התחבורה, בהתאם למכרז ולהסכם מדינת ישראל – משרד התחבורה והבטיחות בדרכים, בביטוח משולב לאחריות מקצועית וחבות המוצר.

14.3.2. הפוליסה תכסה את חבות הספק, עובדיו ובגין כל הפועלים מטעמו:

14.3.2.1. **בקשר עם מעשה או מחדל מקצועי - כיסוי בגין הפרת חובה מקצועית, טעות השמטה, הזנחה ורשלנות.**

14.3.2.2. **חבותו מפגם במוצר - כיסוי בגין נזקים ייגרמו בקשר עם מוצרים שסופקו, תוחזקו, תוקנו, שודרגו, נמכרו, הופצו או טופלו בכל דרך אחרת על ידי הספק או מי מטעמו.**

14.3.2.3. **פעילות הספק, עובדיו ובגין כל הפועלים מטעמו בגין השירותים המפורטים בסעיף 3.1 לעיל.**

14.3.2.4. **גבול האחריות לא יפחת מסך של 10,000,000 ₪ מקרה ולתקופת הביטוח.**

14.3.2.5. **הכיסוי על פי הפוליסה יורחב לכלול את ההרחבות הבאות:**

- הארכת תקופת הגילוי לפחות 12 חודשים.
- מרמה ואי יושר של עובדים.
- אובדן מסמכים, לרבות אובדן השימוש ו/או העיכוב עקב מקרה ביטוח.
- אחריות צולבת - Cross Liability, אולם הכיסוי לא יחול ביחס לתביעות הספק כלפי מדינת ישראל – משרד התחבורה והבטיחות בדרכים.

14.3.2.6. **הביטוח יורחב לשפות את מדינת ישראל – משרד התחבורה והבטיחות בדרכים לגבי אחריותם בגין נזק עקב פגם במוצרים אשר סופקו, שודרגו, הותאמו, עודכנו תוקנו ותוחזקו עבור מדינת ישראל – משרד התחבורה והבטיחות בדרכים, על ידי הספק וכל הפועלים מטעמו ו/או ככל שייחשבו אחראים למעשי ו/או מחדלי הספק וכל הפועלים מטעמו.**

14.4. ביטוח סייבר

14.4.1. הספק יבטח את אחריותו החוקית על פי דיני מדינת ישראל בביטוח חבות סייבר, בין היתר, עקב האירועים המפורטים להלן:

- חבות בדבר הפרת פרטיות כלפי צד שלישי.
- הפרת סודיות כלפי צד שלישי.
- חבות Cyber Security כלפי צד שלישי.
- חבות Media Liability.

14.4.2. הפוליסה תכסה אובדן או נזק סייבר לצד ראשון (הוצאות שהוצאו על ידי המבוטח לצורך שיקום הרשת של המבוטח או לנתונים השמורים ברשת של המבוטח), החלפת חומרה וכן ניהול אירועי סייבר ומשברים, תמיכה ליווי וייעוץ.

14.4.3. גבול האחריות לא יפחת מסך של 10,000,000 ₪ מקרה ולתקופת הביטוח.

14.4.4. הכיסוי על פי פרק החבות כלפי צד שלישי יורחב לכלול:

- סעיף אחריות צולבת, אולם הכיסוי לא יחול על תביעות הספק כנגד מדינת ישראל – משרד התחבורה ובטיחות בדרכים.
- הרחבה לפיה הביטוח יורחב לשפות את מדינת ישראל- משרד התחבורה ובטיחות בדרכים ככל שייחשבו אחראים למעשי ו/או מחדלי הספק והפועלים מטעמו.

14.4.5. הפוליסה תכלול הרחבה בדבר תקופת הגילוי של לפחות 2 חודשים.

14.5. **<u>כללי</u>**

בפוליסות הביטוח הנ"ל הנדרשות יכללו התנאים הבאים:

14.5.1. לשם המבוטח יתווספו כמבוטחים נוספים: **מדינת ישראל – משרד התחבורה והבטיחות בדרכים**, בכפוף להרחבי השיפוי כמפורט לעיל.

14.5.2. בכל מקרה של צמצום או ביטול הביטוח ע"י אחד הצדדים לא יהיה להם כל תוקף אלא, אם ניתנה על כך הודעה מוקדמת של 60 יום לפחות במכתב רשום לחשב משרד התחבורה והבטיחות בדרכים.

14.5.3. המבטח מוותר על כל זכות תחלוף/שיבוב, תביעה, השתתפות או חזרה כלפי מדינת ישראל –משרד התחבורה והבטיחות בדרכים ועובדיהם ובלבד שהוויתור לא יחול לטובת אדם שגרם לנזק מתוך כוונת זדון.

14.5.4. הספק אחראי בלעדית כלפי המבטח לתשלום דמי הביטוח עבור כל הפוליסות ולמילוי כל החובות המוטלות על המבוטח על פי תנאי הפוליסות.

14.5.5. ההשתתפויות העצמיות הנקובות בכל פוליסה ופוליסה תחולנה בלעדית על הספק.

14.5.6. כל סעיף בפוליסות הביטוח המפקיע או מקטין בדרך כל שהיא את אחריות המבטח, כאשר קיים ביטוח אחר לא יופעל כלפי מדינת ישראל, והביטוח הינו בחזקת ביטוח ראשוני המזכה במלוא הזכויות על פי הביטוח.

14.5.7. תנאי הכיסוי של הפוליסות הנ"ל (למעט פוליסת אחריות מקצועית משולבת מוצר ופוליסת סייבר), לא יפחתו מהמקובל על פי תנאי "פוליסות נוסח ביט"ו או נוסח המקביל להם אצל אותו המבטח, בכפוף להרחבת הכיסויים כמפורט לעיל .

14.5.8. חריג כוונה ו/או רשלנות רבתי יבוטל ככל שקיים בפוליסות.

ב. הספק מתחייב בכל תקופת ההתקשרות החוזית עם מדינת ישראל – משרד התחבורה והבטיחות בדרכים, וכל עוד אחריותו קיימת, להחזיק בתוקף את פוליסות הביטוח. הספק מתחייב כי פוליסות הביטוח תחודשנה על ידו מדי תקופת ביטוח, כל עוד החוזה עם מדינת ישראל – משרד התחבורה והבטיחות בדרכים בתוקף.

ג. אישור בחתימתו של המבטח על קיום הביטוחים יומצא על ידי הספק למשרד התחבורה והבטיחות בדרכים, עד למועד חתימת החוזה. הספק מתחייב להציג את האישור חתום בחתימת המבטח אודות חידוש הפוליסות למשרד התחבורה והבטיחות בדרכים לכל המאוחר שבעה ימים לפני תום תקופת הביטוח.
מובהר בזאת כי אישורי הביטוח שיוצגו אינם באים לצמצם ו/או לגרוע מהתחייבויות הספק לערוך את הביטוחים לפי סעיפי הביטוח המפורטים לעיל, ולמען הסר ספק דרישות הביטוח המחייבות הן בהתאם לאמור לעיל. הספק נדרש ללמוד ולעמוד בדרישות אלה ובמידת הצורך להיעזר באנשי ביטוח מטעמו, על מנת לעמוד בדרישות וליישמן בביטוחים כנדרש.

ד. מדינת ישראל – משרד התחבורה והבטיחות בדרכים שומרת לעצמה את הזכות לקבל מהספק בכל עת את העתקי הפוליסות במלואן או בחלקן, במקרה של גילוי נסיבות העלולות להביא לתביעה בפוליסות ו/או על מנת שתוכל לבחון את עמידת הספק בסעיפים אלו ו/או מכל סיבה אחרת, והספק יעביר את העתקי הפוליסות במלואן או בחלקן כאמור מיד עם קבלת הדרישה. הספק מתחייב לבצע כל שינוי או תיקון שיידרש על מנת להתאים את הפוליסות להתחייבויותיו לפי סעיפי הביטוח שלעיל. מוסכם כי הספק יהיה רשאי למחוק מפוליסות הביטוח כאמור מידע עסקי ו/או מסחרי סודי שאינו רלוונטי להתקשרות זו.

ה. הספק מצהיר ומתחייב כי זכות מדינת ישראל – משרד התחבורה והבטיחות בדרכים לעריכת הבדיקה ולדרישת השינויים כמפורט לעיל אינן מטילות על מדינת ישראל – משרד התחבורה והבטיחות בדרכים או על מי מטעמן כל חובה וכל אחריות שהיא לגבי פוליסות הביטוח/ אישורי הביטוח כאמור, טיבם, היקפם ותוקפם, או לגבי העדרם, ואין בה כדי לגרוע מכל חובה שהיא המוטלת על הספק לפי החוזה, וזאת בין אם נדרשו התאמות ובין אם לאו, בין אם נבדקו ובין אם לאו.
למען הסר כל ספק מוסכם בזה כי הביטוחים הנדרשים בנספח זה, גבולות האחריות ותנאי הכיסוי הם בבחינת דרישה מינימלית המוטלת על הספק, ואין בהם משום אישור המדינה או מי מטעמה להיקף וגודל הסיכון לביטוח ועליו לבחון את חשיפתו לסיכונים רכוש וחבות לרבות גוף ורכוש ולקבוע את הביטוחים הנחוצים לרבות היקף הכיסויים, וגבולות האחריות ותקופת הביטוח בהתאם לכך.

ו. אין בכל האמור בסעיפי הביטוח כדי לפטור את הספק מכל חובה החלה עליו על פי דין ועל פי החוזה ואין לפרש את האמור כוויתור של מדינת ישראל – משרד התחבורה והבטיחות בדרכים על כל זכות או סעד המוקנים להם על פי כל דין ועל פי מכרז והסכם זה.

ז. אי עמידה בתנאי נספח זה מהווה הפרה יסודית של חוזה זה.

15. המחאת זכויות או חובות על פי ההסכם

15.1. חל איסור מוחלט על הספק להמחות או להסב כל זכות או חובה על פי הסכם זה או את ביצוע ההסכם, ללא אישור מראש ובכתב של המזמין, בהתאם לשיקול דעתו הבלעדי. מבלי לגרוע מהאמור, המחאת זכויות או חובות לפי הסכם זה תיעשה בכפוף לחתימה על הסכם "גב אל גב" בין הממחה לנמחה. ההסכם האמור יועבר לידי המזמין כתנאי לכניסתה לתוקף של המחאת הזכויות או החובות.

15.2. מוצהר ומוסכם בזה כי למזמין הזכות להמחות או להסב כל זכות או חובה על פי הסכם זה ללא צורך בקבלת אישור כלשהו מהספק או מצד ג' כלשהו.

16. הפסקת ההתקשרות

16.1. המזמין יהיה רשאי להודיע לספק בהודעה מוקדמת של 90 יום על הפסקת ההתקשרות מכל סיבה, בהתאם לשיקול דעתו הבלעדי של המזמין.

16.2. תוקפה של ההתקשרות מותנה בקיומו של תקציב מאושר של המזמין. במקרה שבמהלך תקופת ההתקשרות לא יהיה תקציב מאושר כאמור תופסק ההתקשרות לאלתר.

16.3. מבלי לפגוע בכלליות האמור בכל מקום בהסכם, המזמין רשאי להפסיק את ההתקשרות עם הספק, בהתראה של 30 יום, ולאחר קיום שימוע לספק, בכתב או בע"פ, בהתאם להחלטת המזמין, בהתרחש כל אחד מהמקרים הבאים:

16.3.1. אם ימונה קדם מפרק, מפרק זמני או קבוע לספק;

16.3.2. אם ימונה כונס נכסים זמני או קבוע לעסקי ו/או לרכוש הספק;

16.3.3. אם יינתן צו הקפאת הליכים לספק;

16.3.4. אם ניתן לספק צו לפתיחת הליכים לפי חוק חדלות פירעון ושיקום כלכלי, התשע"ח 2018, או צו שווה ערך במדינה אחרת;

16.3.5. אם הספק פשט את הרגל, חלה במחלה אשר מונעת ממנו את היכולת לבצע את האמור בהסכם זה, או הסתלק מביצוע ההסכם מכל סיבה אחרת;

16.4. על הספק להודיע מידית למזמין על התרחשות אחד המקרים המפורטים בסעיף זה.

17. הפרת ההסכם

17.1. **הפרה יסודית של ההסכם** –

17.1.1. אלה יחשבו כהפרה יסודית של הסכם זה (להלן – "הפרה יסודית"):

17.1.1.1. הפרת סעיפי ההסכם הבאים (לפי כותרת הסעיפים): התחייבויות והצהרות הספק; סודיות; אבטחת מידע; ניגוד עניינים בביצוע ההסכם; קניין רוחני וזכויות יוצרים; קבלני משנה; ערבות ביצוע; הגבלת אחריות; ביטוח; המחאת זכויות או חובות על פי ההסכם;

17.1.1.2. אם הספק לקח חלק בתיאום הצעות, לצורך זכיה במכרז;

17.1.1.3. אספקת מוצר שלא עומד בדרישות ההתקשרות;

אם הספק הסתלק מביצוע ההסכם;

אם נוצר פער טכנולוגי \ כלכלי המשפיע על מימוש ייעודו של מרכז TSOC.

17.1.2. הפר הספק את ההסכם הפרה יסודית רשאי המזמין, לפי שיקול דעתו, לפעול בהתאם למפורט להלן:

17.1.2.1. לאפשר לספק לתקן את הפגם, וזאת תוך 7 ימי עבודה מעת קבלת ההודעה מאת המזמין, או תוך פרק זמן ארוך יותר שיקבע המזמין בהתאם לנסיבות העניין. בכל מקרה בו ההפרה לא תוקנה בפרק הזמן שהגודר לצורך כך, המזמין יהיה רשאי להודיע לספק בהודעה מוקדמת של 7 ימים על הפסקת ההתקשרות.

17.1.2.2. אם כתוצאה מההפרה היסודית המזמין או מי מטעמו צפויים להיפגע באופן מידי, רשאי המזמין להפסיק מיידית את ההתקשרות עם הספק או כל חלק

ממנה ללא התראה מוקדמת ולבטל את ההסכם וזאת מבלי לגרוע מזכות המזמין לסעד או פיצוי כאמור, בהסכם או על פי כל דין.

17.2. הפרת הסכם שאינה יסודית -

המשרד רשאי בכל עת לעכב תשלום בחלקו או בשלמותו אם הפר הספק או איננו ממלא אחד או יותר מתנאי הסכם זה וזאת מבלי לפגוע בזכויותיו של המשרד לפי הסכם זה ולפי כל דין. חישוב הפיצוי המוסכם וקבוע מראש. בגין ביצוע / אי ביצוע כל אחד מהמעשים ו/או המחדלים ישלם הספק למשרד בהתאם למפורט להלן:

מעשה/מחדל	**פיצוי מוסכם**
ניתוק רשתי המביא להשבתת השירות למשך זמן הגבוהה ממה שהוגדר בתוכנית ה ,DRP-ללא יכולת מימוש אתר חלופי.	10,000 ₪על כל מקרה
מוקד לא פעיל כנדרש (איוש חסר, משמרת לא מאויישת בבעלי תפקיד נדרשים על פי המפורט בחוזה.(	10,000 ₪על כל מקרה
קבלת תלונה מאת גוף מנוטר ספציפי, אשר תמצא כמוצדקת, ושעניינה חוסר מקצועיות בניהול אירוע מול הגוף המנוטר.	1,000 ₪לאירוע קל 5,000 ₪לאירוע בינוני 20,000לאירוע חמור (דלף מידע, רשלנות של בקר בעת זיהויי אירוע וכדומה(
איחור בתקופת ההתארגנות (שלא אושר מראש ובכתב על ידי המשרד(	20,000 ₪לכל שבוע איחור
איחור / אי עמידה באבני הדרך והשלבים (שלא אושר מראש ובכתב על ידי המשרד(	20,000 ₪לכל שבוע איחור
הפסקת ההתקשרות ע"י הספק באופן חד צדדי	500,000ש"ח

17.2.1. מבלי לגרוע מהאמור לעיל, בכל מקרה של אי עמידה של הספק בהתחייבויותיו על פי ההתקשרות, מכל סיבה שהיא, המזמין רשאי לאפשר לספק לתקן את הפגם וזאת תוך 15 ימים ממועד משלוח הודעה בכתב מאת המזמין בהתאם להוראות ההסכם, או תוך פרק זמן אחר שיקבע המזמין בהתאם לנסיבות העניין.

17.2.2. בכל מקרה בו ההפרה לא תוקנה בפרק הזמן שהגודר לצורך כך, יהיה רשאי המזמין לפעול בהתאם לתרופות המפורטות להלן:

17.2.3. **ביטול ההסכם עקב הפרה או הפרה צפויה:**

המזמין יהיה רשאי להודיע לספק בהודעה מוקדמת של 30 יום על סיום או השהיית ההתקשרות בגין הפרת ההסכם .

17.2.3.1. נוכח הספק לדעת כי קיימת אפשרות מסתברת כי לא יוכל לעמוד בהתחייבויותיו כולן או מקצתן מכל סיבה שהיא, או כי לא יוכל לעמוד במועדי ובתנאי השירות (בסעיף זה: "**הפרה צפויה**"), יודיע על כך מיד בעל פה ובדואר אלקטרוני למזמין.

17.2.3.2. בכל מקרה של הפרה צפויה של ההסכם, רשאי המזמין לפי שיקול דעתו לאפשר לספק להכין תכנית לתיקון הליקויים ולדון בה, לסיים את ההתקשרות או להשהותה או כל חלק ממנה.

17.2.4. **קיזוז ועכבון** –

17.2.4.1. מבלי לגרוע מזכויות המזמין לפי הסכם זה או על פי כל דין, למזמין תהיה זכות לקזז מסכומים שהוא חב לספק על פי ההסכם, כל חוב שהספק חייב לו, בין קצוב ובין שאינו קצוב, לרבות בין הזמנות. כן יהיו המזמין רשאי לעכב תחת ידו כל סכום שהוא חייב לספק, עד לתשלום כל חוב שיש לספק כלפי המזמין. אם אפשר, יפעל המזמין על מנת לתת אפשרות לספק להשמיע טענותיו לעניין זה.

17.2.4.2. לספק לא תהא כל זכות קיזוז או עכבון כלפי המזמין או מזמין כלשהו בגין כל סכום שלטענתו מי מהם חייב לו.

17.2.5. **חילוט ערבות** –

17.2.5.1. מבלי לפגוע באמור בכל מקום אחר בהסכם, ערבות הביצוע ניתנת לחילוט על ידי המזמין עקב הפרת תנאי ההסכם על ידי הספק או בגין התנהגות שאינה מקובלת ושאינה בתום לב, או לצורך כל תשלום אחר המגיע למזמין מהספק, ובכלל זה פיצויים.

17.2.5.2. לספק תינתן הזדמנות להציג את טענותיו בכתב או בעל פה, בטרם יממש המזמין את סמכותו לפי סעיף זה.

17.2.5.3. במקרה שחילוט הערבות נעשה לצורך פיצוי המזמין, מובהר בזאת כי חילוט הערבות לא ייחשב כתשלום מלוא הפיצויים בהתאם להסכם זה, וכי המזמין יהיה זכאי לקבל מן הספק את ההפרש בין הסכום ששולם עקב חילוט הערבות, ובין סכום הפיצויים המגיעים למזמין.

17.2.5.4. לאחר חילוט הערבות, ובהתאם להנחיות המזמין ולשיקול דעתו הבלעדי, יידרש הספק להעמיד ערבות ביצוע חדשה בסכום הקבוע בהסכם זה, כתנאי להמשך ההתקשרות.

17.2.6. **רכש מספק חלופי** –

17.2.6.1. מבלי לגרוע מהאמור בכל מקום אחר בהסכם ובמכרז, אם כתוצאה מהפרת הסכם או הפרה צפויה, שירות הנדרש למזמין אינו זמין מהספק לשביעות

רצון המזמין, ירכוש אותו המזמין מספק חלופי, בהתאם לשיקול דעתו הבלעדי. אם אפשר, יפעל המזמין על מנת לתת אפשרות לספק להשמיע טענותיו לעניין זה.

18. תרופות מצטברות

18.1. התרופות, לרבות זכות הקיזוז, עיכבון, חילוט, פיצויים מוסכמים, וכל הפעולות שרשאי המזמין בהסכם זה לעשות בתגובה להפרת ההסכם בידי הספק, הן מצטברות, ואין בכל הוראה בהסכם זה כדי לשלול את זכותו של המזמין לכל סעד או תרופה בהתאם להסכם זה או לפי כל דין.

18.2. ויתר המזמין על זכויותיו עקב הפרת הוראה מהוראות הסכם זה על ידי הספק, לא ייחשב כויתור על כל הפרה אחרת של אותה הוראה או הוראה אחרת.

19. סיום התקשרות

19.1. הסתיימה או הופסקה ההתקשרות עם הספק, כולה או מקצתה, מכל סיבה שהיא, יחולו הכללים הבאים:

19.1.1. המזמין ישלם לספק בגין פעולות שביצע הספק טרם הפסקת ההתקשרות, ובגינן זכאי הספק לתשלום בהתאם לכללים המפורטים בהסכם זה.

19.1.2. הספק יידרש לפעול בהקדם וללא דיחוי:

19.1.2.1. להעביר למזמין באופן מסודר את כל תוצרי העבודה שהצטברו אצלו במהלך ההתקשרות.

19.1.2.2. מבלי לגרוע מהאמור לעיל, הספק יעביר למזמין תיק מערכת עדכני כולל יישומים, טבלאות, פיתוחים, ממשקים וכל תיעוד אחר שנערך בקשר למערכת.

19.1.2.3. העברת הנתונים והמידע תבוצע על ידי הספק באופן אשר יבטיח רציפות בשירות, לפי הצורך.

19.1.3. המזמין רשאי להתקשר בהסכם עם ספק אחר בנושא ההתקשרות.

19.1.4. הספק ישתף פעולה עם המזמין בהעברת האחריות בביצוע חובותיו על פי הסכם זה, למזמין או לספק אחר שנבחר על ידי המזמין. בכלל זה יעביר הספק למזמין או לספק החדש כל מידע רלוונטי, יסייע לו במענה לשאלות, ויהיה זמין לפניותיו. במקרה שהספק לא ישתף פעולה בהעברת האחריות, כמפורט לעיל, הוא יישא באחריות על כל נזק שיגרם למזמין או לספק החדש שהחל בביצוע ההסכם. לא ישולם לספק תשלום נוסף עבור שיתוף הפעולה כאמור מעבר לקבוע בהסכם זה.

19.1.5. לא תהיה לספק כל תביעה, דרישה כספית או טענה אחרת כלפי המזמין בקשר עם הפסקת ההתקשרות על פי הסכם זה.

20. כתובות הצדדים והודעות

20.1. כל הודעה על פי הסכם זה תימסר בדואר אלקטרוני, אלא אם הסכימו הצדדים אחרת; הודעה בדואר אלקטרוני כאמור תחשב שנתקבלה עם קבלת אישור קריאה, או לאחר 3 ימים מיום אישור משלוח ההודעה בדואר האלקטרוני, המוקדם מבניהם.

20.2. משלוח דואר אלקטרוני על פי הסכם זה יהיה לכתובת הבאות:

20.2.1. כתובת דוא"ל המזמין: agafcybersec@mot.gov.il או כל כתובת דוא"ל אחרת שתעודכן ע"י המזמין.

20.2.2. כתובת דוא"ל הספק: _____ או כל כתובת דוא"ל אחרת שתעודכן ע"י הספק.

20.3. כל הודעה **מהותית** על פי הסכם זה (כגון הודעות בנוגע לעיכובים, חריגות בתמורה, טענות הפרה, נושאים בעלי דחיפות וכיוצ"ב) תימסר בדואר אלקטרוני אשר ילווה בפנייה טלפונית לצורך וידוא קבלת הדואר האלקטרוני.

20.4. אישור שליחה מתיבת הדואר האלקטרוני, ישמש ראיה למועד השליחה. אישור קריאה, ישמש ראיה לתאריך המסירה.

21. שונות

21.1. הצדדים מסכימים כי סמכות השיפוט בכל הקשור לנושאים והעניינים הנובעים או הקשורים בהסכם זה תהא אך ורק לבתי המשפט המוסמכים במחוז בו יושבת ועדת המכרזים של המזמין, ויחול עליהם החוק הישראלי.

21.2. פרטים מההסכם ומאופן מימושו יפורסמו באתר חופש המידע הממשלתי, זאת בהתאם לנוהל פרסום התקשרויות ובמקרים הרלוונטים גם לפי החלטת ממשלה 1116 מיום 29.12.2013, זאת בהתאם להנחיות המפורטות בהחלטת הממשלה האמורה.

21.3. כל שינוי בהוראת הסכם זה ייעשה בהסכמת שני הצדדים, מראש ובכתב.

21.4. הסכם זה ממצה את כל אשר הוסכם בין הצדדים, ולא יהיה תוקף לכל הסכם או הסדר שנערכו עובר לחתימתו של הסכם זה בנושא ההתקשרות.

21.5. מועד החתימה על ההסכם יהיה מועד החתימה של אחרון הצדדים על ההסכם.

ולראיה באו הצדדים על החתום:

_____ **שם וחתימה** **מורשה חתימה מטעם המזמין** _____ **תאריך**	_____ **שם וחתימה** **מורשה חתימה מטעם הספק** _____ **תאריך**
_____ **שם וחתימה** **מורשה חתימה מטעם המזמין** _____ **תאריך**	_____ **שם וחתימה** **מורשה חתימה מטעם הספק** _____ **תאריך**

נספח ג'– ערבות ביצוע
תדפיס ערבות דיגיטאלית (אין למלא ידנית, למילוי על ידי מערכת)

מסמך זה הוא תדפיס של ערבות דיגיטאלית ונועד לצרכי המחשה בלבד תדפיס זה הופק ע"י המערכת של &שם מנפיק הערבות/מקבל הערבות לפי העניין& ביום DD/MM/YYYY ב- HH:MM:SS על סמך קובץ ערבות דיגיטאלית.

<u>נתוני הערבות</u>

<u>קוד הערבות הדיגיטאלית</u>: XXXX-YYYN-NNNN-NNNN-NNCC

<u>מנפיק הערבות</u>:
_____ מס' סניף: ____
טלפון מנפיק הערבות: _____ פקס' מנפיק הערבות: _____
כתובת מנפיק הערבות: _____
רחוב ומספר: _____ ישוב: _____ מיקוד _____
שם מורשה החתימה 1: _____
שם מורשה החתימה 2: _____

<u>מקבל הערבות</u>:
_____
_____

<u>הנערבים (להלן ביחד ו/או לחוד: "הנערב")</u>:

מזהה נערב	שם הנערב
_____	_____

<u>נושא הערבות</u>:
(שם המכרז / נושא ההתקשרות)

<u>סכומים ותאריכים</u>
סכום הערבות _____ שקלים חדשים.
הצמדה: _____ תאריך בסיס להצמדה: _____
תאריך הנפקת הערבות: _(מילוי על ידי המנפיק)_ תאריך סיום תוקף הערבות: _____

<u>ניסוח ההתחייבות</u>
מנפיק הערבות, ערב בזה כלפי מקבל הערבות, בעבור הנערב, לסילוק כל סכום אשר מקבל הערבות ידרוש מאת מנפיק הערבות, בקשר עם נושא הערבות, ואשר לא יעלה על סכום גובה הערבות. מנפיק הערבות מתחייב בזאת לשלם למקבל הערבות את הסכום האמור בתוך מספר הימים לחילוט הקבועים בערבות וזאת מתאריך דרישת מקבל הערבות ומבלי שמקבל הערבות יהיה חייב לנמק את דרישתו או לדרוש תחילה את סילוק הסכום מאת הנערב.
במקרה של דרישה כאמור מנפיק הערבות לא יטען כלפי מקבל הערבות טענת הגנה כל שהיא שיכולה לעמוד לו או לנערב, ולא יתנה את התשלום בתנאי כלשהו או יעכבו מסיבה כלשהי ובכלל זה בסילוק הסכום האמור מאת הנערב.
ערבות זו אינה ניתנה להעברה או להסבה.
ערבות זו ניתנת למימוש לשיעורין, באופן שחילוטה החלקי לא יגרע מתוקפה לגבי יתרת סכום הערבות שלא חולט, ובלבד שסך כל התשלומים על פי ערבות זו לא יעלה על סכום הערבות.
על ערבות זו יחולו הוראות הדין הישראלי בלבד.
הכללים לניהול כתב ערבות זה יהיו בהתאם לתקן הערבויות הדיגיטאליות כפי שפורסם באתר הוראות התכ"ם של החשב הכללי, כנוסחו במועד הנפקת הערבות, ובכלל זה בהתאם לכללים המפורטים להלן:

- ניהול ערבות זו יעשה באופן דיגיטלי, על ידי שליחת דרישות ובקשות בין מערכות מקבל הערבות ומערכות מנפיק הערבות, בהתאם לכללים המפורטים בתקן הערבויות הדיגיטליות.
- התאריכים בערבות מתייחסים לימים קלנדריים, המסתיימים בשעה 23:59, וזאת למעט מניין הימים לתשלום בגין חילוט ערבות על ידי מנפיק הערבות. מניין הימים לתשלום בגין חילוט הערבות, יחל ביום העסקים הבנקאי בו התקבלה הדרישה לחילוט ממקבל הערבות. במקרה שבו הדרישה התקבלה שלא במהלך יום עסקים בנקאי, מנין הימים לביצוע החילוט יחל ביום העסקים הבנקאי העוקב.
- לאחר שתאריך סיום תוקף הערבות חלף, תוקפה של הערבות פוקע ללא צורך בביצוע פעולה נוספת מטעם הנערב, מקבל הערבות או מנפיק הערבות.

<u>מספר ימים לחילוט 15</u>

<u>אסמכתאות</u> (למילוי על ידי המערכת הטכנולוגית, לא על ידי המשרד)
אסמכתא פנימית של מנפיק הערבות:
אסמכתאות פנימיות 1 של מקבל הערבות:
אסמכתאות פנימיות 2 של מקבל הערבות:
אסמכתאות פנימיות 3 של מקבל הערבות:
אסמכתאות פנימיות 4 של מקבל הערבות:

נספח ד'– התחייבות לסודיות והיעדר ניגוד עניינים

לכבוד
משרד התחבורה

1. אני _____, ת"ז _____, אשר תפקידי אצל _____ *[למלא שם הספק]* (להלן - "**הספק**") הינו _____, נותן התחייבות זו בקשר למכרז אפיון, הקמה והתפעול של מרכז ניטור ותגובה סייבר במגזר התחבורה (TSOC) מספר 11/2026 (להלן - "**המכרז**") .

2. בהתחייבות זו תהיה למונחים הבאים המשמעות המופיעה לצידם:

2.1. "**מידע**" - כל מידע (Information), ידע (Know-How), ידיעה, מסמך, תכתובת, תוכנית, נתון, מודל, חוות דעת, מסקנה וכל דבר אחר כיוצ"ב הקשור באספקת השירותים בין בכתב ובין בע"פ ו/או בכל צורה או דרך של שימור ידיעות בצורה חשמלית ו/או אלקטרונית ו/או אופטית ו/או מגנטית ו/או אחרת.

2.2. "**סודות מקצועיים**" - כל מידע אשר יגיע לידי בקשר לאספקת השירותים, בין אם נתקבל במהלך מתן השירותים או לאחר מכן, לרבות ומבלי לפגוע בכלליות האמור לעיל: מידע אשר ימסר על ידי מדינת ישראל ו/או כל גורם אחר ו/או מי מטעמה.

3. הנני מתחייב לשמור את המידע והסודות המקצועיים שיגיעו אלי עקב ההסכם, בסודיות מוחלטת ולעשות בהם שימוש אך ורק לצורך מילוי חובותיי על פי ההסכם.

4. מבלי לפגוע בכלליות האמור, הנני מתחייב לא לפרסם, להעביר, להודיע, למסור או להביא לידיעת כל אדם את המידע והסודות המקצועיים שהגיעו אלי עקב ההסכם, למעט מידע שהוא בנחלת הכלל או מידע שיש למסור על פי כל דין.

5. לא מתקיים כל ניגוד עניינים בין כל פעילות אחרת או התחייבות אחרת שלי לבין התחייבויות הספק על פי הסכם זה.

6. אמנע מכל פעולה שיש בה כדי ליצור ניגוד עניינים בין מילוי תפקידי על פי ההסכם לבין מילוי תפקיד או התחייבות אחרת, במישרין או בעקיפין.

7. אני מתחייב להודיע למזמין על כל חשש לקיום ניגוד עניינים בין התחייבויותיי על פי ההסכם לבין פעילות אחרת שלי.

שם: _____ חתימה: _____ תאריך: _____

נספח ה'– כללי הצמדה לתמורה

1. הגדרות בנושא הצמדה

1.1. **הצמדה** – הסדר הנעשה בהתקשרות ונועד להתאים ערך נכס, שירות או מחיר, לשינויים ברמת המחירים, בהסתמך על פרסומי הלשכה המרכזית לסטטיסטיקה, בנק ישראל או פרסומים רשמיים ובלתי תלויים אחרים, מישראל ומחוץ לישראל.

1.2. **מדד הבסיס** – המדד הידוע בתאריך הבסיס.

1.3. **מדד קובע** – המדד הידוע בתאריך הקובע.

1.4. **תאריך הבסיס** – נקודת הזמן בה התקבע הערך אשר ביחס אליו תבוצע ההצמדה לאורך תקופת ההתקשרות.

1.5. **התאריך הקובע** – נקודת הזמן שלפיה תחושב ההצמדה בפועל עבור תקופה מוגדרת.

2. תנאי ההצמדה

הצמדה – התמורה עבור רכיב א' (הפניה לעמ'/הצעת המחיר) תהא צמודה לתעריף חשכ"ל מכרז אספקת שירותי מחשוב 16.2.11 או מכרז מקביל שיחליפו ; התמורה עבור רכיבים ב-ד, תהיה צמודה למדד המחירים לצרכן

2.1. תאריך הבסיס – מועד החתימה על הסכם ההתקשרות.

2.2. התאריך הקובע – תאריך קבלת הטובין/ השירותים.

2.3. תדירות ההצמדה – חודשית.

3. ביצוע ההצמדה

3.1. ביצוע ההצמדה יחל מהחשבונית הראשונה להתקשרות.

3.2. אופן חישוב ההצמדה -

3.2.1. ההצמדה לסעיפים ב-ד בטבלת העלות החודשית בפועל תתבצע בהתאם למועד פרסום המדד הרלוונטי. במקרה שהתאריך הקובע אינו יום עדכון המדד, ביצוע ההצמדה יחל ביום עדכון המדד האחרון הקודם לתאריך הקובע.

3.2.2. חישוב ההצמדה יבוצע אחת לתקופה, בהתאם לתדירות ההצמדה הקבוע לעיל.

סכום ההצמדה שיחושב יתווסף או יופחת לתעריפים שנקבעו בהתקשרות.

3.3. מרכיב עלות כח האדם בהצעה יוצמד ויעודכן אל מול העלאות שכר שיבוצעו ובהתאם לעדכון בתעריף חשכ"ל מכרז אספקת שירותי מחשוב 16.2.11 או מכרז מקביל שיחליפו. בהלימה להגדרת התפקידים ודרישות הסף המוגדרים ובכפוף לאישור סגן חשב המשרד.

נספח ו1'– נספח סייבר ואבטחת מידע – רמה רגילה

1. הגדרות ייעודיות לטופס זה:

1.1. <u>אירוע אבטחה</u> – אירוע (incident) אשר עלול לפגוע בזמינות, ברציפות התפעולית, במהימנות או בסודיות המידע של המשרד, של מערכות או קוד המסופקות לו, של חומרה, תכנה, מאגרי מידע או תשתית, שבהם הספק עושה שימוש לצורך ביצוע ההסכם, ובכלל זה תקיפת סייבר.

<u>גורם מנחה</u> – הגורם המנחה את המזמין בהיבטי סייבר והגנות מידע הוא מערך הסייבר הלאומי.

1.2. <u>מזמין</u> – הגוף הרוכש עמו נחתמה ההתקשרות.

1.3. <u>מידע</u> – כל מסמך, תכתובת, תכנית, נתון, עובדה, פרט תוכן, מודל, תמונה, סרט, הקלטה, תהליך עסקי, חוות דעת, קוד ולוגיקה, אשר נשמרו או תועדו על ידי הספק באמצעי טכנולוגי מכל סוג שהוא.

1.4. <u>מידע רגיש</u> – מידע של המזמין אשר יש בחשיפתו כדי לפגוע או לשבש בדרך כלשהי את עבודת המזמין, לפגוע בשירותים המסופקים על ידי המזמין או הממשלה, או לחשוף פרטים ומידע של המזמין אשר אינם נחלת הכלל, ובכלל זה מידע אישי של אזרחים או עובדים, תהליכי עבודה רגישים, שרטוטי מתקנים, תיאור מערכות אבטחה, קוד מקור ותוכנות של מערכות המזמין, מסמכי תכנון של מערכות המזמין או של מערכות המותאמות לשימושו, אמצעי הזדהות ואימות, מידע לגבי מזמינים מסווגים, יעדי הספקה של חומרה או מערכות וכל מידע אחר שיוגדר על ידי המזמין.

1.5. <u>מינהל הרכש</u> – מינהל הרכש הממשלתי באגף החשב הכללי או נציגו.

1.6. <u>שירות חיוני</u> – אחד מאלה:

1.6.1. שירותים המסופקים על ידי המזמין לאזרחי ותושבי מדינת ישראל אשר תפקודם התקין והסדור הוא קריטי לניהול חיי האזרח או לפעילות המשק.

1.6.2. שירות של המזמין הנדרש לתפקודו התקין של המזמין או הממשלה.

1.7. <u>תקיפת סייבר</u> – אירוע אבטחה אשר נוצר כתוצאה מניסיון לעבור או לעקוף את אמצעי האבטחה או הבקרה שבהם הספק או המזמין עושים שימוש, למנוע גישה לשירות או למידע, או לנצל חולשה קיימת בניסיון לגרום להרס, אובדן, דלף, שינוי, שימוש, חשיפה לא מורשית או גישה לנתוני המזמין.

2. כללי

2.1. הספק יהיה האחראי הבלעדי על אבטחת המידע שהועבר או נצבר אצלו במסגרת ההתקשרות. בנוסף, הספק יהיה אחראי על אבטחת המערכות, התוכנות והחומרה המשמשת אותו לצורך אספקת השירותים או המוצרים למזמין, על תקינותם, אמינותם (integrity) ועל תפקודם השוטף והתקין. לצורך עמידת הספק בחובות אלו יתפעל הספק ויעדכן את אמצעי האבטחה באופן שוטף, ויוודא כי האמצעים הטכנולוגיים והתהליכיים המשמשים לאבטחת המידע הם עדכניים ועומדים בסטנדרטים המקובלים בתחום.

2.2. מבלי לגרוע מהאמור, ולצורך עמידה בחובותיו על פי טופס זה, מסכים הספק על שיתוף פעולה עם המזמין כמפורט בטופס זה, והכל לצורך ביצוע תקין של התקשרויות עם ממשלת ישראל.

2.3. מנכ"ל הספק או בעל התפקיד הבכיר בחברה יהיה הכתובת לכל פניה באשר לחובות הספק בהתאם לטופס זה, כמפורט בסעיף 7 להלן, אלא אם מינה נציג אחר מטעמו והודיע על כך בכתב למזמין.

2.4. הספק מתחייב לתקן ליקויים שנמצאו על ידי המזמין בפרק זמן סביר ועל חשבונו, וכן מסכים כי אם לא יתקן ליקויים כאמור בפרק זמן סביר, יהווה הדבר הפרה יסודית של ההסכם, ויהווה עילה להפסקת התקשרות בכפוף לשימוע.

2.5. חובות הספק לפי טופס זה יחולו כל עוד מידע רגיש של המזמין זמין במערכותיו.

3. חובת דיווח

3.1. הספק מתחייב להודיע למזמין, בהקדם האפשרי, במהלך כל שעות היממה ובכל יום בשבוע, וללא שיהוי, על כל אירוע אבטחה אשר מסכן מידע או מערכות של המזמין או עלול להשפיע על יכולתו לעמוד בהתחייבויותיו נשוא ההסכם, ובפרט יודיע למזמין על האירועים הבאים:

3.1.1. אירוע אבטחה או תקיפת סייבר אשר הביאו לדלף מידע הקשור למזמין או לשיבושו של מידע או קוד תוכנה.

3.1.2. אירוע אבטחה או ניסיון תקיפת סייבר אשר עלול להביא לפגיעה במערכות המזמין, במערכות המסופקות לו, במידע של המזמין או בקוד המשמש אותו.

3.1.3. אירוע אבטחה או ניסיון תקיפת סייבר אשר מטרתו לאסוף מידע על המזמין.

3.2. דיווח זה יעשה באמצעות פרטי הקשר של המזמין אשר מפורטים להלן:

03-9545429/30, agafcybersec@mot.gov.il .

3.3. הספק מתחייב להודיע על אירועים כאמור בסעיף 3.1 גם למרכז הארצי לניהול אירועי סייבר (CERT) באחד מהאמצעים הבאים:

3.3.1. חיוג חירום מקוצר למרכז המבצעי לניהול אירועי סייבר במספר 119.

3.3.2. פניה באמצעות הדואר האלקטרוני: 119@cyber.gov.il.

3.4. במקרה כאמור, על הספק להודיע למזמין על התרחשות האירוע ועל כל פרט נוסף ביחס לאירוע זה. **חובה זה תחול גם אם אין ביד הספק את כלל המידע הרלוונטי, ועליו יהיה לעדכן את דיווחיו בהתאם למידע שיצטבר אצלו ולהנחיות המזמין.** על הדיווח לכלול לפחות את הפרטים הבאים:

3.4.1. תיאור כללי של האירוע, אופן התרחשותו, ציר הזמן הידוע של האירוע וכולי.

3.4.2. אופן הטיפול באירוע, והאמצעים הננקטים באופן מידי לצורך צמצום הנזק ומזעור החשיפה בטווח הזמן המידי.

3.4.3. המערכות אשר נפגעו או היו היעד לתקיפה.

3.4.4. המידע אשר זלג, נפגע או שהיה היעד לתקיפה.

3.4.5. ניתוח דרכי התקיפה, החולשות ששימשו את התקיפה וכל מידע רלוונטי אחר.

3.4.6. פעולות מתקנות למניעת הישנות אירועים אלו בעתיד.

3.4.7. כל מידע אחר, שיידרש על ידי המזמין, לצורך ניתוח האירוע.

3.5. חובת הדיווח המפורטת בסעיפים 3.1 – 3.2 לעיל תוגבל למידע הרלוונטי למערכות הספק המשמשות למתן שירותים למזמין או מחזיקות במידע רגיש, ולא נדרש גילוי מידע של לקוחות או גורמים בלתי קשורים אחרים.

4. ביקורת תקופתית

4.1. המזמין יהיה רשאי לבצע, אחת לשנה לכל היותר, ביקורת תקופתית על אודות עמידת הספק בכל דרישות הגנת המידע, הפרטיות והסייבר החלות על אספקת השירותים למזמין. ביקורת זו תתבצע, בתיאום מראש, בדרך של בקשת דוחות ודיווחים על אופן עמידת הספק בדרישות המכרז לאבטחת מידע והגנות סייבר. על הספק להעביר את הדוחות והדיווחים בהתאם ללוח הזמנים שיוגדר על ידי המזמין.

4.2. במקרה שהספק סבור כי יש בהעברת המידע חשש לפגיעה בתהליכי העבודה שלו, או בשירותים הניתנים ללקוחות האחרים שלו או שהיא כרוכה בעלויות כספיות לא פרופורציונאלית, יפנה למזמין לצורך תיאום אופן ביצוע הביקורת.

5. ביקורת בעקבות חשש לתקיפת סייבר

5.1. המזמין יהיה רשאי לבצע ביקורת בעקבות חשש לתקיפת סייבר המשפיע על אספקת השירותים או המוצרים למזמין, בהתאם לאחד המסלולים המפורטים להלן:

5.1.1. מסלול א' – ביקורת על התמודדות הספק

5.1.1.1. המזמין יהיה רשאי לדרוש כל מסמך או פירוט לגבי אופן התמודדות הספק עם תקיפת הסייבר כמפורט בסעיף 3.2 לעיל או כל מידע אחר הנדרש על מנת להעריך את היקף ההשפעה על אספקת השירותים או המוצרים למזמין.

5.1.1.2. המזמין יהיה רשאי לדרוש מהספק לבצע כל בדיקה או פעולה סבירה במערכותיו של הספק המשמשות למתן השירותים לצורך בחינת התקיפה או על מנת לבחון קיום אירוע כאמור. כל מידע שיועבר לספק לצורך בדיקה זו הוא רגיש ואין להעבירו לכל גורם אחר ללא אישור המזמין.

5.1.1.3. במקרה שהמזמין, בהתייעצות עם הגורם המנחה, מצא כי אין די באמור בסעיפים לעיל על מנת להבטיח בצורה מספקת את הגנת המערכות או המידע של המזמין, או שמדובר במידע רגיש, או באירוע שיש לו השפעה על שירותים חיוניים, יהיה המזמין רשאי לקבוע כי במקביל לעבודת הספק, המשך הטיפול באירוע יהיה כאמור במסלול ב' כמפורט בסעיף 5.1.2 להלן.

5.1.2. מסלול ב' – סיוע של המזמין בהתמודדות עם האירוע

5.1.2.1. פעילות במסלול זה תהיה בכפוף להחלטת המזמין ובהתאם לשיקול דעתו הבלעדי, ובכפוף להסכמה מפורשת ובכתב של הספק, למעט במקרים המפורטים בסעיף 5.1.1.3, שבהם לא תידרש הסכמה מפורשת של הספק.

5.1.2.2. המזמין יסייע לספק בביצוע הפעולות המפורטות להלן, באופן ישיר ובאמצעות כלים העומדים לרשות המזמין ועל חשבונו:

5.1.2.2.1. בדיקת מערכות הספק הנוגעות למתן השירותים או לאספקת המוצרים.

5.1.2.2.2. בדיקת הנזקים או הסיכונים שנגרמו למזמין.

5.1.2.2.3. סיוע בהתמודדות עם אירוע האבטחה.

5.1.2.2.4. אבחון אופן התקיפה, המערכות שנפגעו והשפעתה על מתן השירות.

5.1.2.2.5. בחינת דרכים למנוע את המשכם והישנותם של הסיכונים שנגרמו למזמין ומתן הנחיות לספק בדבר הדרכים לצמצם סיכונים אלו וכולי.

5.1.2.3. אין בסיוע על ידי המזמין בכדי להפחית אי אלו ממחויבויות הספק. במקרה שהספק חושב שהנחייה מסוימת עשויה לפגוע ברמת האבטחה או בשירותים הניתנים על ידו, עליו להתריע על כך בצורה מפורשת לנציג המזמין.

5.2. הספק ישתף פעולה כמיטב יכולתו עם דרישות המזמין ויעמיד לרשותו כל מידע נדרש לצורך אבחון והתמודדות עם אירוע האבטחה או על מנת לוודא כי אירוע כאמור לא מתקיים. מידע זה יוגבל למידע הרלוונטי למערכות המזמין או המערכות המשמשות למתן שירותים למזמין, וללא גילוי מידע של לקוחות או גורמים בלתי קשורים אחרים.

5.3. אם הספק סבור כי יש בהעברת המידע או באופן ביצוע הביקורת חשש לפגיעה בתהליכי העבודה שלו או בשירותים הניתנים ללקוחות האחרים שלו, יפנה למנהל מינהל הרכש הממשלתי לצורך תיאום אופן ביצוע הביקורת.

6. נציגי המזמין

6.1. לטובת ביצוע ההתחייבויות המפורטות בטופס זה, המזמין יהיה רשאי להעביר את כלל המידע שהתקבל אצלו לידי הגורם המנחה, וכן לידי מינהל הרכש, וזאת לצורך הערכת סיכונים וקביעת פעולות הנדרשות מהספק.

6.2. הגורמים המנחים את המזמין בהיבטי אבטחת מידע והגנות סייבר ומינהל הרכש יהיו רשאים לבוא במקום המזמין בכל סמכות הנתונה למזמין לפי טופס זה, והספק ישתף פעולה עם הנחיות שיתקבלו מהם לפי הוראות הטופס.

6.3. הגורם המנחה ומינהל הרכש יהיו מחויבים להשתמש במידע שיתקבל מהספק אך ורק לצרכים האמורים בטופס זה תוך גילויו לגורמים הנדרשים לכך בלבד.

7. כתובת לפניות בנושא אבטחת מידע והגנת סייבר

7.1. הודעות/פניות בנושא אבטחת מידע והגנת סייבר יועברו לספק באמצעות כתובת הדואר האלקטרוני הבאה: nt-soc@mot-il.io

חתימת הספק:

_____	_____	_____
שם	תאריך	חתימה