

**מדינת ישראל - משרד האוצר  
 אגף החשב הכללי - מינהל הרכש הממשלתי**

**מכרז מרכזי 05-2022**

**תיחור מס' 5 לאספקת מערכות XDR (Extended Detection & Response)) ושירותים נלווים עבורן**

**גרסה 1 – ספטמבר 2023**

1. כללי התיחור

* 1. כללי
     1. מינהל הרכש הממשלתי באגף החשב הכללי, משרד האוצר (להלן: "עורך המכרז"), מפרסם תיחור לאספקת מערכות XDR – Extended Detection & Response ומתן שירותים עבורן (להלן: "התיחור"). תיחור זה נערך כחלק ממכרז מרכזי 05-2022 לרכש ואספקת מוצרים ושירותים בתחום אבטחת המידע וההגנה בסייבר עבור משרדי הממשלה, יחידות הסמך וגופים נלווים (להלן: "המכרז המרכזי") והוא יסומן כתיחור מס' 5.
     2. רשאים להשתתף בתיחור רק ספקי המסגרת. במסמך זה, יכונו ספקי המסגרת גם כ"מציע".
     3. אין להפיץ את מסמכי התיחור לאף גורם מלבד הגורמים הנדרשים לצורך המענה לבקשה זו ובכפוף להתחייבותו של אותו גורם, לשמירה על סודיות מסמכי התיחור.
     4. את המענה לתיחור זה יש להגיש עד למועד המפורט [בנספח א' – פרטים כלליים לתיחור](#נספח_א).
     5. יובהר כי מסמך תיחור זה הנו חלק בלתי נפרד ממסמכי המכרז ועל ספק המסגרת חלים כל החובות והזכויות המפורטות הן במסמכי המכרז והן במסמך זה.
     6. התיחור יערך בשיטה של תיחור דינאמי מקוון. ככל ששיטת התיחור תשתנה, יודיע על כך עורך המכרז מראש לספקים הרשומים תוך זמן סביר אשר יאפשר הגשת הצעות כספיות לתיחור.
     7. בתיחור זה ייבחר זוכה יחיד (להלן: "הזוכה") אשר יהיה רשאי לספק את כל קו המוצרים והשירותים הכלולים בתיחור זה.
     8. יובהר כי, מזמין שפרסם מכרז או התקשר עם ספק כלשהו לרכישת מוצרים ושירותים נשוא התיחור טרם ההכרזה על הזוכה בתיחור, רשאי להמשיך בהליך המכרזי ובהתקשרות עד תומם בהתאם לתנאים האמורים בהם. כמו כן, מזמין רשאי להתקשר בהתקשרות לרכישת מוצרים ושירותים נשוא התיחור, שלא באמצעות מכרז זה, באישור ועדת הפטור כהגדרתה בתקנות חובת המכרזים, תשנ"ג – 1993.
     9. מובהר בזאת כי עורך המכרז יהיה רשאי לעדכן את מסמך התיחור ונספחיו, על פי שיקול דעתו הבלעדי, זמן סביר לפני המועד האחרון להגשת ההצעות כמפורט [בנספח א' – פרטים כלליים לתיחור](#נספח_א). במקרה כאמור, ישלח עורך המכרז מסמכי תיחור מעודכנים. ככל שפרסם עורך המכרז מהדורה מעודכנת של מסמכי התיחור, על המציע להקפיד על הגשת המענה על פי הנוסח המעודכן.
     10. יודגש, כי הן הספק הזוכה והן היצרן אשר את מוצריו הוא משווק, לא יהיו רשאים לפרסם את עצם התקשרות זו או כל פרט מפרטיה, וכי עורך המכרז שומר לעצמו את הזכות לא לפרסם הוראה פומבית (הודעת תכ"ם) בנושא תיחור זה, אלא להפיצה באופן אחר.
     11. אשת הקשר לתיחור זה היא מיכל קוניוק, כתובת דוא"ל: [GPA\_cyber@mof.gov.il](mailto:GPA_cyber@mof.gov.il).
     12. בכל פנייה בנושא תיחור זה, יש לציין בכותרת המייל את מס' התיחור, שם התיחור ונושא הפנייה (לדוגמא: "תיחור מס' 5 – שירות XDR – שאלות הבהרה").
     13. בהגשת הצעתו, מצהיר ספק המסגרת כי הצעתו עונה על כל דרישות המכרז והתיחור ובכללן: המפרט, תנאי המימוש, זמני אספקה, תקופות התיחור וכו' וכי הוא קרא, הבין וקיבל את דרישות מסמך התיחור ואת תשובת עורך המכרז לשאלות ההבהרה.
  2. שאלות הבהרה והערות
     1. הגשת שאלות הבהרה והערות
        1. שאלות הבהרה והערות לתיחור זה יש לשלוח לכתובת הדוא"ל המפורטת בסעיף ‎1.1.11 לעיל, וזאת עד למועד האחרון להגשת שאלות הבהרה והערות, כמפורט [בנספח א](#נספח_א)' [– פרטים כלליים לתיחור](#נספח_א).
        2. השאלות תוגשנה אך ורק על גבי קובץ ה-Excel המצורף להודעת עורך המכרז על פרסום התיחור (להלן: "**הודעת פרסום התיחור**") ומסומן כנספח א'1.
        3. על ספק המסגרת לוודא באמצעות דואר אלקטרוני חוזר כי קובץ השאלות הגיע לנמען. אי מענה על שאלת הבהרה לא תהווה עילה לאי הגשת הצעה במועד שנקבע.
        4. שאלות שיועברו לאחר המועד או שיופנו בעל פה, בטלפון או בפורמט אחר מהנדרש לא יחייבו מענה על ידי עורך המכרז.
        5. לא יינתן מענה לשאלות שישלחו בעילום שם.
        6. עורך המכרז רשאי לאפשר סבבים נוספים של שאלות הבהרה והערות, בהודעה שתפורסם לספקי המסגרת.
        7. מציע אשר יש לו הערות או טענות לגבי התיחור או תנאיו נדרש להעלותן במסגרת שלב שאלות ההבהרה. יודגש כי לאחר הגשת ההצעה המציע יהיה מושתק ולא יוכל להעלות טענות באשר לתנאי התיחור.
     2. מענה עורך המכרז לשאלות הבהרה והערות
        1. תשובות והבהרות תינתנה בכתב בלבד. נוסחן הוא הנוסח המחייב והן יהיו חלק בלתי נפרד ממסמכי התיחור.
        2. תשובות והבהרות של עורך המכרז, יפורסמו לספקי המסגרת. באחריות ספק המסגרת להתעדכן בתשובות עורך המכרז וכן בעדכונים שוטפים אשר יפורסמו על ידי עורך המכרז בנוגע למכרז והתיחור.
        3. עורך המכרז רשאי לבצע כל שינוי במסמכי התיחור, וכן ליתן פרשנות או הבהרה להוראות המכרז והתיחור, גם ללא קשר לשאלות הבהרה.
        4. עורך המכרז אינו מחויב לנוסח שאלה שהוגשה, ובכלל זה רשאי עורך המכרז, בעת ניסוח מענה לשאלות ההבהרה, לקצר נוסח של שאלה או לנסחה מחדש.
        5. זהות השואלים לא תפורסם במסגרת המענה לשאלות ההבהרה או בכלל, למעט על פי חובה שבדין.
  3. הגשת הצעות
     1. כללי
        1. המציע יגיש הצעה אחת למוצריו ושירותיו של יצרן אחד.
        2. למען הסר ספק, מציע נדרש לעמוד בכל הדרישות המפורטות במסמך זה. אין לשנות את דרישות עורך המכרז. שינוי כאמור עלול להביא לפסילת ההצעה בהתאם לשיקול דעתו של עורך המכרז.
        3. יש לתת מענה לנספחים ב' עד ו' בלבד כאשר אין צורך לחתום על המענה בכל עמוד, ואין צורך לחתום במקום אחר במסמכי המענה, אלא אם כן הדבר צוין מפורשות (כגון בנספח ב').
        4. ההגשה תתבצע לתיבת מכרזים דיגיטלית, כאמור בסעיף ‎1.3.2 להלן.
        5. המסמכים שיוגשו במסגרת המענה לתיבת המכרזים הדיגיטלית:

|  |  |
| --- | --- |
| שם המסמך | הערות |
| אישור המציע | חתום ע"י מורשה חתימה מטעם המציע, בנוסח המצ"ב [כנספח ב'.](#נספח_ב)  יוגש בפורמט PDF. |
| דרישות מקצועיות וטכניות | מענה מלא לשאלות המפורטות [בנספח ג'](#נספח_ג) המצ"ב. ניתן להגיש את המענה הן בעברית והן באנגלית.  יוגש בפורמט Word. |
| מחירון | המחירון הרשמי של היצרן. על המחירון הרשמי להיות חתום כנדרש בסעיף 3.7 למסמכי המכרז המרכזי.  יוגש בפורמט PDF. |
| מפרט רישוי | מפרט רישוי מלא של היצרן עבור כל המוצרים הכלולים במחירון הרשמי שלו.  יוגש בפורמט PDF. |
| מודל ייחוס | מענה מלא על מודל הייחוס בהתאם למפורט בנספח ד'1 המצורף להודעת פרסום התיחור. יש לשים לב להוראות סעיפים 3.7.4 ו-3.7.5 למסמכי המכרז המרכזי.  יוגש בפורמט Excel. |
| הצהרת יצרן | הצהרה עבור היצרן אשר מוצרים מתוצרתו מוצעים במכרז, בהתאם לנוסח המצ"ב [כנספח ה'](#נספח_ה). ניתן להגיש את ההצהרה בשפה העברית או האנגלית.  יוגש בפורמט PDF. |
| בקשה לחיסיון פרטים מתוך ההצעה | בנוסף לאמור בתחילת נספח ו', ככל שהמציע סבור כי בהצעתו יש חלקים שהם בגדר סוד מסחרי או סוד מקצועי, עליו למלא את הטבלה המצ"ב [כנספח ו'](#נספח_ו).  יוגש בפורמט Word. |
| מינוי נציג למערכת מיר"ב | רק במקרה שהמציע מבקש לשנות את הנציג מטעמו יגיש את הנוסח המצורף כנספח 1 לחוברת מס' 2 למסמכי המכרז המרכזי.  יוגש בפורמט PDF. |
| מסמכים נוספים | ניתן לצרף נספחים למענה, ככל שהדבר נדרש, לרבות , אישורים, פרוספקטים וכד'.  מסמכים כאלו, יוגשו בפורמט בו נערכו במקור- למשל, Excell. |

* + 1. הגשת הצעות בתיחור
       1. מציע המעוניין להשתתף בתיחור יגיש את המענה שלו, כמפורט לעיל, לתיבת המכרזים הדיגיטלית, באמצעות מערכת הגשת הצעות מקוונת.
       2. קישור למערכת הגשת ההצעות יפורסם לספקי המסגרת לפחות חמישה ימי עבודה טרם המועד האחרון להגשת הצעות.
       3. המועד האחרון להגשת הצעות לתיבת המכרזים הדיגיטלית מפורט [בנספח א](#נספח_א)' להלן.
       4. לצורך הגשת הצעתו יידרש המציע להזדהות באמצעות מערכת ההזדהות הממשלתית ולבצע רישום מוקדם למערכת הגשת ההצעות.
       5. לאחר ביצוע ההזדהות יש לוודא כי מופיעים במערכת להגשת ההצעות פרטי התיחור הרלוונטי.
       6. במסגרת הגשת ההצעה על המציע לפעול בהתאם להנחיות שיופיעו במערכת הגשת ההצעות, למלא את כלל השדות שנדרש באופן ברור ובהתאם להנחיות המערכת, ולהעלות למערכת את הקבצים הנדרשים בהתאם להוראות המכרז והתיחור.
       7. לאחר השלמת הגשת ההצעה במערכת יופיע במסך ההגשה מספר אסמכתא. ככל שלא התקבל מספר אסמכתא ההצעה לא הוגשה.
       8. לא ניתן יהיה להגיש הצעות במערכת לאחר המועד האחרון להגשת הצעות.
       9. **באפשרות המציע לבצע הגשה אחת בלבד**! **לאחר השלמת הגשת הצעה לא תתאפשר הגשה נוספת או עדכון הצעה.**
       10. ככל שתהיה תקלה טכנית, אשר תמנע הגשת הצעות במכרז, יוכל עורך המכרז בהודעה שתפורסם באתר האינטרנט לקבוע דרך הגשה אחרת במכרז.
       11. תנאים נוספים לשימוש במערכת הגשת ההצעות:
           1. הגודל המרבי לכל קובץ בהצעה הינו 10 MB ומקסימום 50 MB לכלל הקבצים ביחד באותה הצעה. על המציע לבדוק את גודל הקבצים הנשלחים על ידו ולוודא כי הצעתו עומדת במגבלות.
           2. ניתן להעלות למערכת קבצים מסוג PDF / WORD / EXCEL.
           3. קיימת מגבלה על מס' התווים בשם הקובץ שמועלה – 64 תווים לכל היותר.
           4. סיוע טכני: בסוגיות טכניות ובעזרה בתפעול המערכת ניתן לפנות למוקד התמיכה בימים א'-ה' בין השעות 8:00-17:00 באמצעות קישור זה: <https://merkava.mrp.gov.il/ccc/index.html>. יש לציין בפניה את שם המכרז, המועד האחרון להגשת ההצעות ובמידת הצורך לצרף צילומי מסך. זמן ההמתנה מרגע משלוח הפניה ועד לחזרת נציג שירות לא יעלה על 4 שעות בטווח שעות פעילות המוקד. במקרים חריגים בלבד ייתכן וזמן ההמתנה יחרוג מ-4 שעות. מוקד התמיכה אינו מתחייב לספק מענה לפניות אשר יתקבלו בזמן קצר מ-4 שעות מהמועד האחרון להגשת הצעות.
           5. **בחלוף 20 דקות ללא ביצוע פעולה, המערכת תתנתק וכל פעולה שבוצעה בה ולא נשמרה כטיוטה, לא תשמר**. במקרה המתואר תידרש כניסה מחודשת למערכת.
           6. להנחיות וחומרי הדרכה על אופן הגשת ההצעות בתיבת המכרזים הדיגיטלית ניתן להיכנס לקישור הבא: [https://portal.gpa.gov.il/supplier/tender](https://portal.gpa.gov.il/supplier/tender/).
       12. על המציע 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 ממנו להגיש את הצעתו. **על המציע להיערך לכך, ולהגיש את הצעתו מבעוד מועד**. למציע לא תהיה כל טענה כלפי עורך המכרז באשר לתקלה שהתגלתה במערכת הגשת ההצעות סמוך למועד האחרון להגשת הצעות, גם אם כתוצאה מכך הוא לא הצליח להגיש את הצעתו.
  1. הליך בדיקת ההצעות
     1. ההצעות לתיחור ייבחנו בהתאם לכללים המפורטים במסמכי המכרז המרכזי, בדגש על "חוברת מס' 2 למסמכי המכרז: הנחיות לגבי חלק ב' של המכרז" (להלן: "חוברת מס' 2 למסמכי המכרז המרכזי").
     2. שלב ראשון - חישוב ציון איכות
        1. לתיחור זה נקבע ציון איכות מינימלי, כמפורט ב[נספח א'](#נספח_א). כמו כן, מפורטים בנספח א' המשקלות למתן ציון האיכות במסגרת התיחור. הצעות שיזכו לציון איכות הנמוך מציון האיכות המינימלי שנקבע בנספח א' לא יעברו לשלב התיחור הדינאמי.
        2. לאחר מתן ציוני האיכות לכלל ההצעות בתיחור ולצורך שקלול ההצעות, ההצעה בעלת ציון האיכות הגבוה ביותר תקבל ציון איכות משוקלל של 100, ואילו יתר ההצעות יקבלו ציון יחסי בהתאם ליחס ציון האיכות של הצעתם לציון ההצעה האיכותית ביותר, בהתאם לנוסחה הבאה:

ציון האיכות המשוקלל של ההצעה הנבחנת = ציון האיכות של ההצעה הנבחנת חלקי (÷) ציון האיכות של ההצעה שקיבלה את ציון האיכות הגבוה ביותר מבין כל ההצעות לאותו תיחור, כפול 100. לדוגמה, אם ציון ההצעה האיכותית ביותר הינו 90 וציון ההצעה הנבחנת הינו 72, אזי ציון האיכות המשוקלל של ההצעה הנבחנת יהיה:

* + 1. שלב שני – חישוב מחיר משוקלל
       1. המציעים שהצעותיהם עמדו בתנאי הסף ובציון האיכות המינימלי, לפי העניין, יוזמנו להשתתף בשלב התיחור הדינאמי המקוון, במועד הרשום [בנספח א'](#נספח_א).
       2. התיחור הדינאמי המקוון ייערך במערכת תיחורים חדשה – מערכת מיר"ב (להלן: "**מערכת מירב**") במודל תיחורים אנגלי (הסבר על מודל זה ניתן למצוא בנספח 2 לחוברת 2 למסמכי המכרז המרכזי). עורך המכרז יערוך הדרכה על מערכת מירב טרם קיום התיחור הדינאמי המקוון למציעים המעוניינים בכך.
       3. מועד ההדרכה על מערכת מירב יישלח בדוא"ל לכל ספקי המסגרת.
       4. אופן הרישום ודגשים לשימוש במערכת מירב מפורטים [בנספח ז'](#נספח_ז).
       5. בתיחור הדינאמי המקוון יזין המציע כדלהלן:
          1. אחוז הנחה ממחיר המחירון הרשמי לכלל המוצרים המוצעים על ידי המציע בתיחור.
          2. עלויות עבור שירותי תחזוקה כמפורט בסעיפים הרלוונטיים [בנספח ד'](#נספח_ד) (עלות תחזוקה, עלות שעות עבודה וכו'), והכל בהתאם למפורט בנספח.
       6. רכיבים אלו ישוקללו במהלך התיחור כמפורט במודל הייחוס (נספחים ד', ד'1).
       7. המחיר המשוקלל של ההצעה בתיחור הדינאמי המקוון לא יעלה, בכל מקרה, על המחיר המירבי להצעה כפי שנקבע בהתאם לאמור בסעיף ‎1.4.5.4 להלן.
       8. במידה והמחיר המשוקלל של ההצעה יהיה גבוה יותר מהמחיר המירבי שנקבע להצעה, יקפיא עורך המכרז את התיחור, יתריע על כך בפני המציע ויאפשר לו לתת הצעה נוספת. אם לא ייתן המציע הצעה כאמור, יפסיק עורך המכרז את השתתפות המציע בתיחור ויראה זאת כהפרת התחייבויות המציע.
       9. המחיר הסופי לכלל המוצרים הרלוונטיים אצל היצרן יהיה מחיר המחירון הרשמי בניכוי אחוז ההנחה שניתן על ידי המציע למוצרים. יובהר כי בסיום התיחור יהיה רשאי הספק הזוכה להציע הצעת מחיר משופרת.
       10. במקרה בו זכה המציע בשני תיחורים או יותר, וקיימים פריטים המשותפים לשני תיחורים או יותר, יקבע המחיר הנמוך מבין המחירים המוצעים למוצר.
       11. על ספקי המסגרת המעוניינים בהדרכה נוספת על מערכת התיחורים הדינאמיים (מעבר להדרכות היזומות אליהן זומנו) להודיע על רצונם זה יחד עם מסמכי המענה לבקשת התיחור.
    2. שלב שלישי - קביעת ציון מחיר
       1. מהמחיר המשוקלל של ההצעה ייגזר ציון המחיר בהתאם לנוסחה הבאה:
       2. הגדרות:

– ציון המחיר של מציע

– המחיר המשוקלל של מציע

– המחיר המשוקלל הנמוך ביותר שהתקבל על ידי מי מהמציעים.

– הערך החציוני מבין המחירים הכוללים שהוגשו על ידי המציעים שעמדו בדרישות סעיף ‎1.4.3.1 לעיל, במענה על מודל הייחוס (במקרה של מספר זוגי של הצעות מחיר, יחושב הממוצע של שתי ההצעות האמצעיות).

* + 1. שלב רביעי - חישוב ציון ההצעה ודירוג ההצעות
       1. ציון המחיר ישוקלל יחד עם ציון האיכות המשוקלל של ההצעה בהתאם למפורט בסעיף ‎1.4.5.2 להלן, ויהווה את ציון ההצעה. ההצעות ידורגו בהתאם לציון ההצעה שקיבלו, כאשר ההצעה בעלת הציון הגבוה ביותר תדורג ראשונה. ציון ההצעה ייקבע בהתאם לנוסחה הבאה:
       2. *הגדרות:*

– ציון ההצעה של מציע

– ציון האיכות המשוקלל של מציע

– ציון המחיר של מציע

– משקל האיכות

– משקל המחיר

* + - 1. להלן המשקלות בתיחור זה:

|  |  |
| --- | --- |
| **רכיב** | **משקל** |
| משקל האיכות () | 60% |
| משקל המחיר () | 40% |

* + - 1. **מחיר מירבי**
         1. עורך המכרז יהיה רשאי, טרם ביצוע התיחור הדינאמי המקוון, לקבוע מחיר מירבי להצעה. במקרה זה המחיר המירבי יהיה זהה עבור כלל המציעים.
         2. המחיר המירבי יועבר למציעים לפחות 7 ימי עבודה טרם מועד התיחור הדינאמי המקוון.
         3. לאחר קבלת המחיר המירבי, המציע יהיה רשאי להסיר את הצעתו לתיחור מבלי שהאמור יחשב כאי עמידה בתנאי המכרז. הסרת הצעה כאמור, תבוצע בכתב תוך 2 ימי עבודה ממועד שליחת המחיר המירבי למציע. מציע שלא הסיר הצעתו כאמור, מסכים למחיר המירבי האמור ולהמשך השתתפותו בהליך התיחור.
      2. **תיחור מדמה**
         1. תיחור מדמה ייערך בהתאם למפורט בסעיף 2.9.4 לנספח 2 לחוברת 2 למסמכי המכרז המרכזי.
         2. התיחור המדמה יתקיים במועד המפורט [בנספח א'.](#נספח_א)
         3. ההשתתפות בתיחור המדמה הינה חובה ומהווה תנאי להשתתפות המציע בתיחור הדינאמי המקוון.
         4. ככל שעורך המכרז יחליט על שינוי פרט מסוים בכללי התיחור, ולעמדתו של עורך המכרז יש בשינוי כדי לשנות באופן משמעותי את ההתנהלות במהלך התיחור, יוכל עורך המכרז להכריז על עריכת תיחור מדמה נוסף. במקרה כאמור הכללים המפורטים לעיל יחולו בשינויים המחויבים.
    1. הצעה יחידה
       1. מבלי לגרוע מהאמור בסעיף 1.5.2 למסמכי המכרז המרכזי, ככל שהוגשה בתיחור הצעה יחידה, או שלאחר בדיקת ההצעות נותרה הצעה אחת בלבד, עורך המכרז, בהתאם לשיקול דעתו הבלעדי יהיה רשאי:
          1. להכריז על המציע שנותר כזוכה;
          2. לבטל את התיחור, ולצאת לתיחור חדש;
  1. פרטי ההתקשרות
     1. על ההתקשרות במסגרת תיחור זה יחולו הכללים המפורטים בפרק 3 למסמכי המכרז המרכזי – אופן ביצוע ומימוש ההתקשרות. להלן יפורטו תנאים ייחודיים לתיחור זה.
     2. תקופת ההתקשרות
        1. תקופת ההתקשרות מכוח התיחור (להלן: "**תקופת ההתקשרות בתיחור**") תהיה למשך 36 חודשים מיום הודעת עורך המכרז לזוכה בתיחור על תחילת תקופת ההתקשרות. לעורך המכרז תהיה אופציה להאריך את ההתקשרות בתקופות נוספות עד ל-36 חודשים נוספים (סה"כ 72 חודשים), וזאת בהודעה מוקדמת בכתב של לפחות 15 ימים לפני תום כל תקופה. לאורך כל תקופת ההתקשרות בתיחור, המזמינים יהיו רשאים לרכוש את המוצרים והשירותים מהספק הזוכה.
        2. 21 ימי העבודה הראשונים של תקופת ההתקשרות בתיחור יוגדרו כתקופת התארגנות, במהלכה הספק הזוכה יידרש להשלים היערכותו לקראת אספקת המוצרים והשירותים המבוקשים.
     3. אחריות ותחזוקה
        1. מבלי לגרוע מהאמור בסעיף 3.13.1 למסמכי המכרז המרכזי, תקופת האחריות, השירות והתחזוקה, או תקופת המינוי (Subscription) הראשונה למוצרים והשירותים הנרכשים (לרבות הרחבות, רישוי, דמי מינוי לשירות זה או אחר ותוכנות הכלולות במכירת המוצרים) תהיה כלולה במחיר המוצר או השירות ותעמוד על 12 חודשים מיום **הפעלת המוצר** (Activation), וככל שהמזמין רכש שירותי התקנה והטמעה, מיום אישור המזמין כי ההתקנה, אותה ביצע הספק בפועל, נעשתה לשביעות רצונו ובאופן הנדרש, לפי המאוחר (להלן: "**תקופת האחריות הראשונה**"). במקרה בו לדעת עורך המכרז חל עיכוב בקבלת אישור המזמין מסיבות שאינן תלויות בספק, תחל תקופת האחריות מיום השלמת כל מחויבויותיו של הספק הניתנות לביצוע, בהתאם לקביעת עורך המכרז.
        2. הספק הזוכה יספק תקופות אחריות ותחזוקה נוספות, מעבר לתקופת האחריות הראשונה, בתעריף שהוצע על ידו במסגרת הצעתו בתיחור ולכל היותר, עד 72 חודשים ממועד תום תקופת ההתקשרות בתיחור (להלן: "**תקופת האחריות והתחזוקה**"). קרי, חובת האחריות והתחזוקה יכולה להימשך גם לאחר תום תקופת ההתקשרות.
        3. יובהר כי, אם מודל המכירה הינו במינוי (Subscription), שירותי האחריות והתחזוקה יינתנו במחיר המינוי, לכל אורך תקופת המינוי (גם אם תקופה זו חורגת מתקופת ההתקשרות), כל עוד המזמין ישלם עבור המינוי ולא תידרש כל עלות נוספת עבור אחריות ותחזוקה גם במקרה של חידוש המינוי.
        4. הרחבת שירות לשירות 24/7
           1. המזמין יוכל לבחור האם הוא מבקש לקבל שירותי אחריות ותחזוקה בחלון קריאה של 24/7, בהתאם לרמת השירות המפורטת בסעיף 3.13.6.3.5 למסמכי המכרז המרכזי.
           2. עבור הרחבת רמת שירות זו, תשולם לספק תוספת תמורה בהתאם למפורט להלן:

עבור מוצר או שירות ברכישה – תמורה בשיעור של 15% ממחיר התחזוקה השנתית כפי שהוצעה בהצעתו – לדוגמה, עבור מוצר שעולה 5,000$, ועלות האחריות והתחזוקה השנתית הינה 10% ממחיר הרכישה, תשולם לספק תמורה של 75$ עבור כל שנה בתקופת האחריות הראשונה, ותמורה כוללת של 575$ עבור כל שנת אחריות ותחזוקה נוספת (עלות תחזוקה שנתית לכל אחת מהשנים הנוספות הינה 10%X5,000=$500, תוספת התמורה עבור הרחבת השירות הינה 15%X500=75$).

עבור מוצר או שירות במינוי (Subscription) – תמורה בשיעור של 5.25% מעלות המינוי השנתי – לדוגמה עבור מוצר שעולה 1,500$ לשנה, יקבל הספק תשלום של 78.75$ עבור כל שנה בה השירות נדרש (5.25%X1,500=78.75$).

* + - * 1. יובהר כי מזמין יוכל להפעיל ולהפסיק את הרחבת השירות בכל עת, כאשר הפסקת השירות תיכנס לתוקף במלאת שנה קלנדרית מהפעלת ההרחבה.
    1. רישוי
       1. במקרה של שינוי ארגוני (לרבות פיצול או איחוד משרדים או יחידות), המזמין יהיה רשאי להמיר כל רישוי, לרישוי מקביל אצל אותו המזמין או להעביר רישוי למזמין אחר, וזאת תוך הודעה על השינוי האמור לספק.
       2. הרישוי לצורך הקמת מעבדת בדיקה יהיה ללא עלות ויוגבל ל-30 יום.
       3. על היצרן להחזיק ממשק ניהול רישיונות הניתן לגישת כלל המזמינים באמצעות רשת האינטרנט בו המזמין, לאחר זיהויו, יכול לקבל דיווח על כלל הרישיונות שרשומים בארגונו, תוקפם, תוקף הסכם התחזוקה וכד'. מזמין יוכל לבקש כי זיהויו לא יופיע במערכת והספק ימנע מלהעלותו למערכת ככל והדבר נדרש מראש, או למוחקו ממנה בהתאם לנדרש תוך 5 ימי עבודה. לחלופין, ובהסכמת המזמין, ניתן לשנות את זיהוי המזמין לזיהוי אחר המתואם עם המזמין.
       4. עלות הרישוי בהקמת DR פאסיבי או להקמת "מערכת רדומה" (Active-Standby) יהיה 20% מעלות הרישוי כפי שנקבעה בתיחור.
    2. התקנת והטמעת המוצרים והשירותים הנרכשים
       1. המזמין רשאי לרכוש כחלק מהמוצרים והשירותים המבוקשים, גם שירותי התקנה והטמעה, וזאת בהתאם לאמור בסעיף 3.8.4 למסמכי המכרז המרכזי ולמפורט [בנספח ד'](#נספח_ד).
       2. ככל שהמזמין רכש שירותי התקנה והטמעה, ייערך הספק, בתיאום עם המזמין, להקמת הפרויקט ולביצוע העבודות הנדרשות ולצורך כך יתאם עם המזמין את תכולות העבודה בהתאם למפורט בסעיפים 3.9.8-3.9.6 למסמכי המכרז המרכזי, ובהתאם למפורט להלן.
       3. במסגרת התקנת והטמעת המוצרים והשירותים, ככל ושירותים אלו הוזמנו על ידי המזמין, יגדיר הספק את כלל ההגדרות הנדרשות, בהתאם למפורט במסמכי המכרז, להנחיות המזמין, ול-Best Practice של היצרן עד לתפעול מלא ותקין של המוצר.
       4. בנוסף, ידריך הספק את אנשי המזמין לתפעול מלא ועצמאי של המערכת כך שבסיום הליך ההתקנה וההטמעה, יהיה בידי הצוותים המקצועיים של המזמין הידע הנדרש לתפעול המוצר באופן שוטף, מלא ועצמאי.
    3. התמורה עבור התקנת והטמעת המוצרים והשירותים הנרכשים
       1. עבור כל שעת התקנה והטמעה שבוצעה בפועל (להלן: "**שעת עבודה"**)יקבל הספק תמורה בסך של 250 ₪ (כולל מע"מ) לשעת עבודה.
       2. התמורה עבור שעות עבודה שבוצעו מעבר לשעות העבודה המקובלות תהיה בכפוף לאמור בסעיף 3.8.4.4 למסמכי המכרז המרכזי.
       3. תעריף שעת העבודה יתעדכן, לכל היותר אחת ב-12 חודשים, בהתאם לשינוי האחוזי שיחול בתעריף של בעל תפקיד "מיישם הגנת סייבר" ברמת התמחות ב', כפי שנקוב בטבלת "תעריפים מירביים" בהודעת התכ"ם הנלווית למכרז 01-2009 להספקת שירותי מחשוב למשרדי הממשלה (נכון למועד פרסום התיחור, מס' ההודעה הוא 16.2.11 ל"הספקת שירותי מחשוב למשרדי הממשלה" – <https://takam.mof.gov.il/document/HM.16.2.11> או בכל הודעה שתחליף אותה (להלן: "**מכרז שירותי מחשוב**").
       4. ככל והתעריפים במכרז שירותי מחשוב יעודכנו, על הספק לפנות לעורך המכרז ולבקש ממנו לעדכן את תעריף שעת העבודה. נכון למועד פרסום התיחור, התעריף הרלוונטי בהודעה הוא 204 ₪ (לא כולל מע"מ) לשעה.
          1. להלן דוגמא לאופן ביצוע ההצמדה: אם תעריף "מיישם הגנת סייבר ברמת התמחות ב' יעל-220 ₪ במהלך ההתקשרות, כלומר עלייה של 7.84%, יוכל הספק, בחלוף 12 חודשים מתחילת ההתקשרות או ממועד שינוי התעריף הקודם (המאוחר מביניהם), לבקש את העלאת התעריף לשעת עבודה לסך של 269.6 ₪ (כולל מע"מ). עדכון זה יחול על הצעות המחיר שיוצעו מיום אישור עדכון התעריף ולא יחול על הצעות שהוגשו למזמינים או על הזמנות שבוצעו.
       5. במקרה שיחולו שינויים במכרז שירותי מחשוב או תיערך התקשרות מרכזית אחרת בנושא, ובהתאם לכך תימחק/תשתנה הגדרת התפקיד "מיישם הגנת סייבר" או שיימחקו/ישתנו רמות ההתמחות, עורך המכרז רשאי, בהתאם לשיקול דעתו הבלעדי, לבחור סוג תפקיד אחר ורמת התמחות אחרת לצורך יישום מנגנון העדכון.
    4. צוות נותני השירותים
       1. בנוסף על האמור בסעיף 3.6.2.2.2 למסמכי המכרז המרכזי, מזמין יהא רשאי לדרוש מהזוכה להחליף מיישם בכל עת ומכל סיבה סבירה, והזוכה יקצה מיישם אחר במקומו עבור המזמין תוך 21 ימי עבודה.
    5. רשימת המוצרים המאושרים לרכישה
       1. רשימת המוצרים המאושרים לרכישה בנושא התיחור תיקבע על ידי עורך המכרז בהתייעצות עם המועמד לזכייה טרם תחילת תקופת ההתקשרות בתיחור. במהלך תקופת ההתקשרות, ובהתאם לצרכי המזמינים, עורך המכרז יעדכן את רשימת המוצרים המאושרים לרכישה בנושא התיחור. על רשימת הפריטים המאושר בנושא התיחור יחולו אחוזי ההנחה שנקבעו בתיחור. אם ליצרן מוצרים או שירותים בנושא התיחור, המתאימים להתקנה מקומית (On Premises), עורך המכרז יהיה רשאי להוסיפם לרשימת המוצרים לרכישה כמפורט לעיל. אולם, על פריטים אלו לא יחולו אחוזי ההנחה שנקבעו בתיחור, אלא, יתקיים לגביהם משא ומתן ובכל מקרה, אחוזי ההנחה על פריטים אלו, לא יפחת מאחוז ההנחה שנקבע בתיחור.
       2. בנוסף לאמור לעיל, לעורך המכרז שמורה הזכות לאחר התיחור ובמהלך כל תקופת הרכש להוסיף לתכולת ההתקשרות מוצרים ושירותים שאינם בתחום מושא התיחור ואשר נדרשים לצורך ייעול ומקסום השימוש בפריטים בתחום התיחור, בין היתר, מבין הקטגוריות:
       3. התקנות, תחזוקה, שירות והדרכות נוספות.
       4. אפליקציות ותוכנות מתממשקות.
       5. חומרה להרצה מובנית של השירותים בתחום התיחור.
       6. מחיר הפריט שהתווסף יקבע במסגרת מו"מ בין עורך המכרז לספק הזוכה, בשים לב למחיר הפריט או השירות בארץ או בחו"ל, מחירון היצרן, מחירוני יצרנים אחרים, תוך שקלול תנאי השירות הרלוונטיים למכרז, אופי הפריט והשימוש בו.
       7. היקף הרכש של הפריטים שיתוספו במהלך תקופת ההתקשרות, לא יעלו במצטבר, על שיעור של 20% מהיקף הרכש שיתבצע מכוח התיחור.
    6. עיבוד ואבטחת מידע והגנה בסייבר בשירותים
       1. בנוסף על האמור במסמכי המכרז [ובנספח ג'](#נספח_ג) למסמך התיחור, מפורטים ב[נספח ח'](#נספח_ח) כללים הנוגעים לאופן אספקת השירותים.
       2. כללים אלו יחייבו את הספק והיצרן המוצע מטעמו ביחס לאספקת השירותים במסגרת התיחור.
    7. ערבות ביצוע
       1. בהתאם לסעיף 11 להסכם ההתקשרות ולסעיף 2.12.3 לחוברת מס' 2 למסמכי המכרז המרכזי, המועמד לזכייה יידרש להעמיד ערבות ביצוע על סך: 500,000 ₪. הערבות תהיה ערבות דיגיטאלית בהתאם לסעיף 11.3.2. למסמכי המכרז המרכזי.
       2. הערבות תעמוד בתוקף עד ל-90 ימים מתום תקופת הרכש או תקופת האחריות והתחזוקה האחרונה, לפי המאוחר מביניהן.

1. נספח א' – פרטים כלליים לתיחור

|  |  |
| --- | --- |
| **מופע בתיחור** | **מועד** |
| מועד אחרון להגשת שאלות הבהרה והערות | 22.10.2023 |
| פרסום עורך המכרז מענה לשאלות הבהרה | לפחות 12 ימים לפני המועד האחרון להגשת הצעות |
| מועד פתיחת תיבת המכרזים הדיגיטלית להגשת הצעות | 12.11.2023 בשעה 9:00 |
| מועד אחרון להגשת הצעות | 19.11.2023 בשעה 13:00 |
| תוקף הצעה לתיחור | 19.5.2024 |
| מועד תיחור מדמה (להצעות שעמדו בדרישות התיחור) | יישלח בנפרד |
| מועד תיחור דינאמי מקוון (להצעות שעמדו בדרישות התיחור) | יישלח בנפרד |

* 1. **מועדים בתיחור**
     1. מועדים אלו הינם לידיעה בלבד ואינם מהווים אישור לתקינות ההצעה ולהשתתפות בתיחור הדינאמי המקוון.
     2. השתתפות מציע בתיחור הדינאמי המקוון מותנית בהודעת ועדת המכרזים על אישור הצעתו להשתתפות בתיחור.
     3. תוקף ההצעה רשום בטבלת התאריכים לעיל. עורך המכרז רשאי להודיע על הארכת תוקף ההצעה לתקופה נוספת של עד 90 ימים (ובהסכמת ספק המסגרת אף מעבר לכך), זאת עד לבחירת זוכה. המציע אינו רשאי לחזור בו מהצעתו בתקופה האמורה.
  2. **ציון איכות מינימלי ומשקלות למתן ציון**
     1. ציון האיכות המינימלי שנקבע עבור תיחור זה לצורך מעבר לשלב התיחור הדינאמי המקוון, הוא 80% **(אחרי נטרול רכיב "הערכת היקף ויכולת מרכז פיתוח בארץ").** כמו כן, ציון האיכות המינימלי שנקבע עבור משקלת "הערכת אופן המימוש בענן, ההגנה בסייבר, אבטחת מידע ופרטיות בפתרון המוצע", הוא 85%.
     2. להלן יפורטו המשקלות לצורך מתן ציון האיכות:

|  |  |  |  |
| --- | --- | --- | --- |
| **מס"ד** | **נושא** | **משקל** | **ציון איכות מינימלי** |
|  | הערכת קו המוצרים המוצע (היקף המערכת המוצעת, יכולות המערכת, תצורת מימוש המערכת, תמיכה בתשתיות ענן שונות, ביצועים, התאמה לסטנדרטים פתוחים, גמישות המערכת והתאמתה למבני פעולה שונים, היקף מערכת הניהול, יכולות שילוב והתאמה למערכות קיימות ומשיקות, הערכת קלות ומהירות הטמעה, יכולות נוספות מעבר לנדרש, היקף קו המוצרים וכד'). | 40% |  |
|  | הערכת אופן המימוש בענן, ההגנה בסייבר, אבטחת מידע ופרטיות בפתרון המוצע (אופן מימוש הפתרון בענן, המשכיות עסקית ו-SLA, הגנת ואבטחת תהליכים ותשתיות, הגנה על המידע של המזמינים וכד'). | 15% | 85% |
|  | הערכת היצרן (מעמד בשוק, הערכת גופי מחקר, מדיניות דיווח ושקיפות, ניסיון מוכח, מערך התמיכה, הסמכות ועמידה בתקנים וסטנדרטיים ישראליים ובינלאומיים, רוחב פתרונות האבטחה של היצרן וממשקים עם מוצרים משיקים וכד'). | 10% |  |
|  | הערכת היקף ויכולת מרכז הפיתוח בארץ (במקרה של התחייבות היצרן להקמת מרכז כאמור במקרה של זכייה במכרז, יינתן ניקוד חלקי). | 15% |  |
|  | הערכת יכולת המציע (ניסיון בתחום ובתחומים דומים, מס' עובדים בתחום, הכשרות רלוונטיות וכד'). | 20% |  |
| **סה"כ** | | 100% | **80%**  (למעט רכיב "הערכת היקף ויכולת מרכז פיתוח בארץ") |

1. נספח ב' – אישור המציע

אנו, מורשי חתימה מטעם \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, מאשרים בחתימתנו כי:

[שם המציע]

1. קראנו את מסמכי התיחור, לרבות הנספחים להם.
2. כל סעיף במסמכי התיחור מובן ומקובל עלינו והמציע יהיה מנוע ומושתק מלעלות טענות כנגד תנאי התיחור מרגע הגשת הצעה לתיחור.
3. הפרטים המופיעים בהצעה זו על נספחיה הם אמת, והמציע מסוגל ומתכוון לעמוד בכל פרט מהצעתו ובהוראות המכרז והתיחור.
4. הצעה זו, על כל פרטיה, מולאה באופן עצמאי ע"י המציע, ללא התייעצות, הסדר או קשר עם מציע אחר.

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  תאריך | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  שם מלא | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  תפקיד אצל המציע | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  חתימה וחותמת |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  תאריך | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  שם מלא | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  תפקיד אצל המציע | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  חתימה וחותמת |

**(ניתן לחתום באמצעות חתימה אלקטרונית, ובלבד שחתימה זו מבטיחה כי היא נעשתה על ידי המורשה הרלוונטי וכי לא נעשה שינוי בקובץ לאחר חתימתו.)**

4. נספח ג' – דרישות טכניות

* 1. **הנחיות למענה על נספח זה**
     1. סעיפים בהם ישנה דרישה לפירוט בלבד **אינם מהווים דרישת חובה**, ועל המציע לפרט באופן ברור את יכולות היצרן או הפתרון המוצע, אם יכולות אלו נתמכות במענה המוצע. יובהר, כי אי מענה לסעיף מסוג זה יתקבל כחוסר תמיכת הפתרון המוצע ביכולות המפורטות בסעיף.
        1. אם סעיפים אלו אינם מתקיימים בפתרון המוצע במועד האחרון להגשת הצעות, אך יש צפי לקיומם, יש לציין לוח זמנים.
     2. סעיפים בהם קיימת דרישה מפורשת לתכונה או יכולת, **הינם סעיפי חובה,** ולא תתקבל הצעה שאינה כוללת מענה לדרישה או ליכולת המפורטת בסעיף. ככל שבסעיף נדרש פירוט לגבי אופן המענה, על המציע לספק פירוט כנדרש.
        1. אלא אם נקבע אחרת בסעיף ספציפי, המערכת המוצעת נדרשת לעמוד בכל סעיפי החובה המפורטים בנספח זה, **נכון** למועד האחרון להגשת הצעות בתיחור.
     3. **יובהר כי, כל הסעיפים המפורטים בנספח ג' יכללו במסגרת הערכת ההצעות וניקודן.** לכל תכונה או יכולת נתמכת, נדרש מענה מפורש האם יכולת או תכונה זו כלולה בפריטים המוצעים במודל הייחוס, או האם נדרש רכש או רישוי נוסף על מנת לממשם.
     4. **יודגש, כי חוסר תשובה, תשובה שאיננה עונה לדרישה, חוסר מענה לדרישה, או תשובה לא ברורה ולא חד משמעית, עלולים להביא לניקוד נמוך של ההצעה או לפסילתה של ההצעה והכל בהתאם לשיקול דעתו הבלעדי של עורך המכרז.**
     5. מענה לנספח זה ניתן להגיש הן בשפה העברית והן בשפה האנגלית.
  2. **תנאים ודרישות לגבי היצרן והמציע**
     1. בנוסף לקיום מוקד שירות פעיל ע"י המציע כמפורט בסעף 3.13.6.2 מסמכי המכרז המרכזי, היצרן יידרש לספק מרכז תמיכה שישמש כתובת לפניות ושאלות מקצועיות (להלן: **"מרכז התמיכה"**), דרכו ניתן יהיה לקבל מענה תוך 24 שעות באמצעות אחת או יותר מהאפשרויות הבאות: (**א**) מענה טלפוני הפעיל בשעות העבודה המקובלות, כהגדרתן בסעיף 3.10.1 למסמכי המכרז המרכזי. (**ב**) פורטל לפתיחת פניות שירות. (**ג**) כתובת דוא"ל ייעודית לצורך מכרז זה. על המציע לפרט על הסכם אמנת השירות של היצרן (SLA), אופן ההתקשרות, הכתובת/טלפון ואופן הפעלת המוקד. עורך המכרז רשאי לקבוע כללים לגבי אופן הפנייה למרכז התמיכה.
     2. מרכז התמיכה נדרש לספק תמיכה בשפה האנגלית. נדרש פירוט לגבי יכולת תמיכה בשפה העברית.
     3. הזוכה יידרש לספק מסמכי המלצת יצרן (Best Practices) להקשחות והגדרות הגנה מומלצות מטעמו למוצר ה-XDR, בדגש על אופן השימוש במוצר על מנת להגיע לסטנדרט אבטחה מקובל כדוגמת ISO-27002, NIST ו-CIS.
     4. על המציע לפרט את מדיניות היצרן בנוגע לשקיפות ודיווח היצרן על בעיות/חשיפות אבטחתיות שהתגלו במוצריו בתחום מושא התיחור, או לגבי כל פרצה או חשיפת מידע אחרת ממערכותיו, לרבות פרק הזמן לדיווח על כך.
     5. מקום פיתוח המוצר:
        1. המציע יפרט את מיקום פיתוח המוצרים והמערכות בתחום מושא התיחור. יש לצרף אישור יצרן בהתאם.
        2. אם היצרן מתחייב להקים מרכז פיתוח בארץ בתחום מושא התיחור, יש לספק פירוט על כך ולצרף התחייבות של היצרן בהתאם.
     6. פרטים לגבי ניסיון המציע במוצר המוצע:
        1. נדרש פירוט על ניסיון המציע במוצר המוצע, לרבות שנת התחלת העבודה עם היצרן המוצע, הלקוחות בהם ביצע המציע התקנה של המוצר המוצע ופירוט המערכות שהותקנו, רמת ההסמכה של המציע מטעם יצרן המערכת המוצעת וכל מידע אחר רלוונטי.
        2. נדרש פירוט של כלל המיישמים המועסקים מטעם המציע להם הסמכה של היצרן למוצרים והשירותים המוצעים בתיחור לפי הפורמט הבא:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| מס' | שם העובד | שנות ניסיון במוצר | ההסמכה למוצרים המוצעים | שנת קבלת ההסמכה | סיווג בטחוני ככל וישנו |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |

* + 1. למציע מוקד שירות פעיל כמפורט בסעיף 3.13.6.2. למסמכי המכרז המרכזי.
    2. על המציע לספק פירוט לגבי אופן התמיכה שלו בשירותים המפורטים להלן:
       1. מתן ייעוץ וסיוע בהגדרת הפתרון המוצע אצל המזמינים – יש לפרט את אופי השירותים המוצעים.
       2. מתן עזרה באתר מזמין – יש לפרט את תהליכי הסיוע והאסקלציה.
       3. מתן הכשרה מקצועית לאנשי הלקוח הכוללת הדרכות והסמכות פורמליות על ידי גורמים המוסמכים על ידי היצרן – יש לפרט את סוגי הקורסים וההסמכות הניתנות הן על ידי המציע והן על ידי היצרן.
  1. דרישות מהמערכת/מוצרים
     1. מוצר **Extended Detection & Response (XDR)** לעניין תיחור זה הינו כלל הכלים והטכנולוגיות תחת פלטפורמה אחת המספקים זיהוי, מניעה, חקירה ותגובה בזמן אמת לאיומים והתקפות מתקדמות על נקודות הקצה (Endpoints) בסביבת הארגון.
        1. לעניין זה, יובהר כי נקודות קצה יכולות להיות תחנת עבודה, מחשב נייד, שרת, רכיב ענן, מכשיר נייד וכדומה.
     2. המערכת והרישיונות המוצעים במודל הייחוס יכללו את כלל הדרישות המפורטות בנספח זה, ללא תוספת תשלום, כולל יכולות התממשקות למוצרי הצד השלישי הנדרשים במסמכי התיחור.
     3. הצעת המציע תכלול את כלל הרכיבים הנדרשים למתן מענה לדרישות מסמכי המכרז המרכזי והתיחור, המפרטים ומודל הייחוס. המציע, בהצעתו לתיחור, מתחייב כי כל המוצרים והשירותים המוצעים על ידו בתיחור מצויים בייצור שוטף, ואין בידיו או בידי היצרן כל מידע או חשש מהפסקת מכירה, ייצור, אספקה או תמיכה של המוצרים והשירותים (או רכיבים או פריטים המשמשים אותם) המוצעים על ידו.
     4. יש לוודא כי הצעת המציע לכל אחד מהרכיבים הנדרשים במודל הייחוס (סעיף ‎4.3.7) כוללת את כל הרישוי הנדרש להפעלת המערכת והשימוש בה.
     5. יש לצרף מפרט רישוי ברור ומובן לכל רכיב מוצע בהתאם למודל הייחוס, וכן לציין את מודל הרישוי (Perpetual, Subscription וכו').
     6. יש לצרף מסמך Best Practice של היצרן בנוגע לניהול ואופטימיזציה של הרישיונות ותפעולם.
     7. להלן פירוט המוצרים הנדרשים:
        1. **מוצר XDR תוכנתי בענן (SaaS):**

| **נושא** | **מענה המציע** | **הערות** |
| --- | --- | --- |
| רישיון XDR ענני (SaaS) בעבור תמיכה וניהול בלפחות 50,000 נקודות קצה |  | יש לתת פירוט לכלל הפריטים הנדרשים למתן המענה.  החישוב יהיה לפי נקודות קצה. אם מחירון היצרן מבוסס על משתמשים ולא נקודות קצה, ובמקרה בו רישיון משתמש כולל לפחות 3 נקודות קצה, לצורך החישוב, ניתן להניח יחס המרה של 1.25 נקודות קצה לכל משתמש (לדוגמא: 50,000 נקודות קצה = 40,000 משתמשים).  כמות זו הינה כמות מוערכת לכלל המזמינים.  נא תשומת לבכם לסעיף ‎5.5.1 בנספח ד' להלן. |
| מערכת ניהול מרכזית |  | מערכת הניהול תתמוך באופן מובנה בכל הרכיבים המסופקים במסגרת ההזמנה עבור משרד ספציפי, ללא כל מגבלה על סוג הרכיבים או כמותם.  מערכת ניהול זו תהיה כלולה במחיר הרישוי. |

* 1. דרישות טכנולוגיות
     1. **מאפיינים כלליים**
        1. תצורת מערכת XDR
        2. המענה נדרש לכלול פתרון XDR בענן (SaaS) בפלטפורמה של יצרן יחיד ותחת מערכת ניהול אחודה לכלל רכיבי המערכת.
           1. נדרש פירוט לגבי תמיכת היצרן ביכולת ומוכנות הפעלת השירות מאזור ענן ציבורי ב"איזור הישראלי" תוך 12 חודשים מיום הודעת הזכייה ובהתאם לדרישות המפורטות בפרק ‏‎4.7 תשתית המערכת.
           2. סוכן המערכת (Agent) יותקן ויגן על נקודות הקצה (End points) בסביבת הלקוח וינוהל על ידי מערכת ניהול מרכזית בענן.
           3. על המערכת להיות מסונכרנת מול מקור זמן מהימן. על המציע לפרט את אופן סנכרון השעון, מקור הזמן, ואופן ההגנה על סנכרון זה מפני שיבוש.
           4. נדרש פירוט על פלטפורמות הענן הציבורי אשר על גביהן ניתן השירות, האם תומכים בענן פרטי (VPC), אופן השמירה על חשאיות ובטחון המידע, אופן ניהול המוצר וכו'.
        3. תצורות נוספות למערכת XDR
           1. נדרש פירוט לגבי תמיכת המערכת בתצורה היברידית הכוללות רכיב מקומי וענני במקביל.
        4. נדרש פירוט לגבי תמיכת המערכת בהתקנה מקומית Self-hosted/On-Premise בסביבת הלקוח כדוגמת שרת וירטואלי (Virtual Appliance). יש לפרט לגבי כלל הדרישות בהיבט התשתית הטכנולוגית הנדרשת להקמת המערכת המוצעת בסביבת הלקוח. הפירוט יכלול כמות וסוגי שרתים נדרשים, רכיבי רשת, מערכות הפעלה, רכיבי אבטחת רשת, סוגי Database, זיכרון וגודל אחסון נדרש.
        5. נדרש פירוט לגבי תמיכת המערכת בתצורת Open XDR המאפשרת יכולת פעולה הדדית עם כלי אבטחה ופלטפורמות אחרות באמצעות ממשקי API.
        6. נדרש פירוט לגבי תצורות נוספות בהן ניתן לרכוש את המוצרים המוצעים.
        7. נדרש פירוט לגבי שירותים וכלים מובנים או נוספים כחלק מפתרון ה-XDR מאת היצרן המוצע כגון שירותי ,MDR מודיעין סייבר וכדומה.
     2. **אופן הפעולה**
        1. על המערכת לתמוך בארכיטקטורתMulti-Tenancy לטובת ניהול מרכזי של המערכת כספק אבטחה (MSSP) למול לקוחות מרובים (פנימיים וחיצוניים לארגון) באופן היררכי ורוחבי עם יכולות הפרדה לוגית וניהול נפרד לכל אחד מהלקוחות. נדרש פירוט לגבי אופן המענה.
        2. נדרש פירוט לגבי אופן פעולת מערכת ה-XDR, ארכיטקטורת המערכת, סוג התשתיות עליהן היא עובדת, אופן איסוף המידע, עיבודו ושמירתו באופן מאובטח.
     3. **תמיכה בנקודות קצה (Endpoints)**
        1. על המערכת לתמוך בהתקנת סוכן (Agent) על סביבות העבודה הבאות:
        2. מחשבים עם מערכות הפעלה Windows 7,8,10,11.
        3. שרתים עם מערכות הפעלה Windows Server 2008, 2012, 2016, 2019, 2022.
        4. שרתים ועמדות קצה עם מערכת הפעלה Linux.
        5. סביבות עבודה וירטואלית VDI - בתצורת תחנה ייעודית (persistent).
        6. סביבות עבודה וירטואלית VDI – בתצורת תחנה צפה (non-persistent).
        7. נדרש פירוט לגבי תמיכה ביכולות הבאות:
        8. הגנה על סביבות עבודה Terminal Server / Citrix Thin Client / וכדומה.
        9. מערכות הפעלה ורכיבים נוספים (כגון ,Kubernetes, MacOS IoT).
        10. יכולת פעילות עצמאית (Standalone) של הסוכן ללא תלות בענן היצרן.
        11. נדרש פירוט לגבי כלל מערכות ההפעלה והגרסאות הנתמכות להפעלת סוכני המערכת, לרבות מערכות הפעלה Legacy כגון Windows XP.
        12. נדרש פירוט לגבי יכולות המערכת, אם קיימות בתצורה חסרת סוכן ((Agentless.
     4. **ביצועים**
        1. המערכת נדרשת לעמוד בזמינות שירות של לפחות 99.95% Uptime. נדרש פירוט לגבי נתוני הזמינות בהם עמד בפועל היצרן במהלך 12 החודשים האחרונים.
        2. על המערכת לכלול יכולת ניטור רציף למצב תקינות שירותי המערכת (Health Monitor) לרבות מצב קישוריות ותקינות הסוכנים (Agents).
        3. נדרש פירוט לגבי אופן השפעת סוכן המערכת על הביצועים וצריכת המשאבים בנקודות הקצה (זיכרון, מעבד, תקשורת, רוחב פס וכדומה).
        4. נדרש פירוט לגבי יכולות הגדרת הסוכן לניצול מינימלי של משאבי המערכת ורוחב פס.
     5. **שרידות, גיבוי ורציפות תפקוד**
        1. המערכת נדרשת לתת שירות בתצורת זמינות גבוהה High Availability. נדרש פירוט לגבי אופן שרידות המערכת.
        2. על המערכת לכלול סביבת DR המאפשרת המשכיות עבודה בעת תקלה מערכתית, אירוע סייבר או אסון, תוך פריסתה בלפחות שני Availability Zones. נדרש פירוט לגבי אופן המענה.
        3. נדרש פירוט לגבי תמיכת המערכת ביכולת גיבוי הגדרות תצורה. יש לפרט את סוג המידע המגובה והאם המערכת תומכת בניהול גרסאות תצורה.
        4. נדרש פירוט לגבי תמיכת המערכת בייצוא הגדרות תצורה לרכיב חיצוני, וכן בייבוא/שחזור הגדרות המערכת.
     6. **שפה**
        1. המערכת נדרשת לתמוך בשפה האנגלית. יש לפרט לגבי תמיכה בשפות נוספות.
        2. נדרש פירוט לגבי תמיכה בשפה העברית בתרחישים כגון:
        3. יבוא/יצוא מזהים (IOC's) דוגמת שמות מתחם בעברית (IDN).
        4. ביצוע שאילתות מול אובייקטיבים בעברית דוגמת מזהים ושמות נכסים.
        5. הפקת דוחו"ת עם אובייקטיבים בעברית דוגמת מזהים ושמות נכסים.
     7. **אבטחת המערכת**
        1. הכניסה למערכת נדרשת לתמוך במנגנון הזדהות אחודה (SSO) ובמנגנון אימות רב-גורמי (MFA), נדרש פירוט לגבי כלל מנגנוני ופרוטוקולי ההזדהות הנתמכים במערכת.
        2. המערכת נדרשת לתמוך באופן מובנה בעבודה עם SAML 2.0 ו-ADFS.
        3. על המערכת לכלול רישום ותיעוד מסודר ורציף ללוג (Log) של כל גישה, שינוי הגדרות ופעילות משתמשים וקבצים במערכת.
        4. קבצי הלוג במערכת יהיו מוגנים מפני גישה (צפייה, שינוי, מחיקה) לא מורשית.
        5. על המערכת לכלול תמיכה בהעברת ושידור קבצי לוג ואירועים למערכות אוטומציה וניטור אבטחתי כגון SIEM ו- SOARבפורמטים מקובלים כגון Syslog. נדרש פירוט לגבי אופן המענה.
        6. נדרש פירוט לגבי תמיכת המערכת בהעברת ושידור קבצי לוג במקביל למספר מערכות.
        7. על המערכת לכלול תמיכה בהגנה על הסוכן בתחנה (Anti-Tamper) מפני תקיפה, שינוי, עצירה, הסרה מחיקה וכדומה. נדרש פירוט לגבי אופן המענה.
        8. היצרן נדרש לביצוע יזום ותקופתי של מבדקי חדירה (PT) אפליקטיביים על ידי גוף המתמחה בביצוע מבדקים מסוג זה וכן סקרי קוד (Code Review). נדרש פירוט בנוגע למדיניות היצרן.
        9. נדרש להציג דו"ח עדכני של מבדק חדירה וסקר קוד תקין של המערכת מטעם היצרן, בשלב הזכייה ומידי שנה, בהתאם לדרישת עורך המכרז.
        10. נדרש פירוט בנוגע לתמיכה ביכולת החלת מדיניות סיסמאות למשתמשי המערכת (לרבות משתמשים מקומיים), אשר תכלול קביעה של משתנים כגון: אורך, מורכבות, תוקף, היסטוריית סיסמאות, אכיפת MFA וכדומה.
        11. נדרש פירוט לגבי תמיכת המערכת בשמירה ואחסון קבצי הלוג ומידע היסטורי של המערכת לאורך זמן ובזמן מוגדר (לטובת ארכיון, תחקור וכדומה).
        12. נדרש פירוט לגבי יישום עקרונות מודל Zero Trust באמצעות המערכת.
        13. נדרש פירוט לגבי מנגנוני ניטור, אבטחה ונהלי הקשחה עבור כלל הכלים הכלולים במערכת, בדגש על האפליקציה, מאגרי מידע, קישורים מאובטחים.
        14. נדרש פירוט לגבי יכולות המערכת להתמודדות עם מתקפות (כגוןbrute-force ,DDoS וכדומה) וכן לפירוט בנוגע ליישום עקרונות להיערכות, ניהול ותגובה לאירועי אבטחה (IR).
     8. **הרשאות גישה**
        1. המערכת נדרשת לאפשר הרשאות גישה מצומצמות ככל האפשר (least privilege) לביצוע פעולות מורשות למשתמשי המערכת, ובכדי להגן על הנתונים מפני גישה לא מורשית, חשיפה, שיבוש, שינוי או מחיקה. נדרש פירוט לגבי אופן ביצוע הגבלת הרשאות הגישה בפתרון המוצע.
        2. על המערכת לכלול מנגנוני ניהול הרשאות ובקרת גישה מבוססת תפקידים כגון RBAC/ABAC. נדרש פירוט לגבי אופן המענה בנושא זה.
        3. נדרש פירוט לגבי סוגי התפקידים (Roles) הקיימים במערכת לבקרת גישה.
        4. נדרש פירוט לגבי סוגי החוקים (Rules) המובנים הקיימים במערכת להגבלת גישה.
        5. נדרש פירוט לגבי פרמטרים אשר לפיהם ניתן לקבוע מדיניות הרשאות גישה לפעולות השונות ולהגביל דינמית גישת משתמשים למערכת כדוגמת סוג משתמש, תאריך, יום, שעת גישה, כתובת IP, נכס מטרה, מיקום גאוגרפי וכו'.
     9. **תקנים ופרטיות**
        1. על המערכת לתמוך בתקן ISO 27001 ובתקן אבטחת פרטיות בענן ISO .270018 נדרש פירוט של רשימת ההסמכות, התקנים והסטנדרטים הבינ"ל הנוספים בהן עומדת המערכת המוצעת כדוגמת, ISO27017 SOC2 Type II CSA STAR, FedRAMP, GDPR MITRE ATT&CK Evaluation וכו'.
        2. כל המידע הנשמר במערכת, יאוחסן בצורה מוצפנת כאשר מנגנון ההצפנה יתבסס על אלגוריתמים מוכרים ותקניים. נדרש פירוט לגבי אופן מימוש המענה.
        3. המערכת נדרשת לספק למזמין יכולת שליטה על הנתונים שלו, לרבות הזכות לגשת אליהם, להשתמש בהם ולמחוק אותם.
     10. **הצפנה**
         1. על המערכת לתמוך בתקשורת מוצפנת למול כלל רכיבי וממשקי המערכת הפנימיים והמנוהלים לרבות בסיסי נתונים, עמדות קצה, שרתים וכדומה. נדרש פירוט לגבי אופן המענה.
         2. על המערכת לתמוך בתקשורת מוצפנת למול כלל רכיבי המערכת החיצוניים לרבות מאגרי מידע חיצוניים של היצרן ושל ספקי צד ג'. נדרש פירוט לגבי אופן המענה.
         3. כל הנתונים הנשלחים מהסוכן למערכת יעברו בתווך מוצפן (In transit) והמידע יישמר במערכת באופן מוצפן במנוחה (At Rest). נדרש פירוט לגבי אופן מימוש המענה.
         4. על המערכת לתמוך בתקן FIPS 140-2 level 2 ומעלה עבור המודולים הקריפטוגרפים של המערכת. נדרש פירוט לגבי אופן הפתרון.
         5. נדרש פירוט לגבי תמיכה בממשק שורת פקודה (CLI) לניהול המערכת באמצעות פרוטוקול SSH והגישה לממשקים אלו.
         6. נדרש פירוט לגבי תמיכת המערכת בהתממשקות לשירותי KMS בייבוא ניהול מפתחות ההצפנה של המזמין.
     11. **פלטפורמה וממשק**
         1. המערכת תסופק עם פלטפורמה אחודה בממשק WEB מאובטח לניהול ותפעול כלל פעולות ורכיבי המערכת. נדרש פירוט לגבי כלל סוגי ממשקי המשתמש הקיימים לניהול פלטפורמת ה-XDR כגון ממשק ,WEBקליינט ייעודי ו-API.
         2. נדרש פירוט לגבי אופן הגישה לממשקי הניהול, האם יש צורך בגישה לפורטל הנמצא ברשת האינטרנט או שניתן לגשת לממשק הניהול ללא ניתוב פתוח לאינטרנט (כגון VPC Peering).
  2. **מאפייני רכיבי המערכת**
     1. **יכולות זיהוי** 
        1. על המערכת לכלול יכולות גילוי, זיהוי וסיכול בזמן אמת של:
        2. קבצי הרצה זדוניים בשלב טרום הרצה (Pre-execution).
        3. נוזקות מבוססי מזהים/חתימות.
        4. נוזקות ללא מזהה/חתימה ונוזקות מסוג Fileless.
        5. תקיפות מבוססת הסלמת הרשאות (Privilege escalation) והתפשטות רוחבית (Lateral Movement).
        6. גישה בזמן אמת לקישורים זדוניים, כתובות IP ודומיינים חשודים בעלי מוניטין נמוך.
        7. על המערכת לכלול יכולות ניתוח היוריסטי (Heuristic) לקבצים כדי לקבוע את מטרתם, יעדם ושימושם.
        8. המערכת נדרשת לנטר ולדווח בזמן אמת על אירועים וממצאים שהתגלו. במידה ונקודת קצה אינה יכולה לדווח באופן מידי על ממצאים, המערכת תאחסן את התוצאות באופן מקומי עד שניתן יהיה להעלות אותן למערכת הניהול המרכזית.
        9. על המערכת לכלול יכולת בניית תרחישי פעולות תגובה (playbooks) בפני איומים וסיכונים כגון, בלימת פעילות קובץ, כיבוי נקודת קצה, ניתוק נקודת קצה מהאינטרנט, הכנסה קבצים להסגר (quarantine) , מחיקת קבצים זדוניים וכדומה. נדרש פירוט לגבי יכולות המערכת.
        10. על המערכת לכלול תמיכה ביכולת הרצה בזמן אמת של קבצים בסביבה בטוחה ומבודדת (Sandbox) לשם איתור אנומליה וסממני פריצה (Indicators of Compromise – IOCs) בפעילות. נדרש פירוט לגבי אופן המענה לנושא זה בדגש על שמירה והגנה על חשאיות המידע.
        11. על המערכת לתמוך בהתממשקות למערכות Sandbox של ספקי צד ג' ובניתוח קבצים גדולים וחשודים.
        12. נדרש פירוט לגבי מיקום וארכיטקטורת שירות ה-Sandbox מטעם היצרן, האם הוא מוגדר כחלק מובנה במערכת או שהינו שירות חיצוני למערכת.
        13. נדרש פירוט לגבי תמיכת המערכת בהתממשקות ל-Sandbox מקומי (On-premise) בסביבת המזמין.
        14. נדרש פירוט לגבי תמיכה בהגדרת חוקי מדיניות לקביעת סוגי הקבצים המאושרים לעלות למערכת ה-Sandbox. לדוגמה, הגדרת מדיניות המאשרת העלאת קבצי הפעלה בלבד וחוסמת העלאת קבצים מכל סוג אחר (כגון מסמכים).
        15. נדרש פירוט לגבי תמיכת המערכת ביכולת הגדרת ואכיפת חוקי DLP עבור העלאות קבצים ל- Sandbox. לדוגמה, לפני העלאת כל קובץ לבדיקה בסביבת ה- Sandbox תתבצע בדיקת תאימות לעמידה במדיניות הארגון כדי לוודא שהקובץ אינו מכיל פרטים אישיים/נתונים רגישים.
        16. על המערכת לכלול יכולת חיפוש בכל נקודות הקצה של מזהים (IOCs) או תכונות מערכת אחרות (כגון שם קובץ, נתיב קובץ, דומיין, כתובת יעד, מזהה Hash וכדומה).
        17. נדרש פירוט לגבי תמיכת המערכת בממשק למערכות הלבנה לקבצים (CDR) וביצוע הרצה של תהליך בזמן אמת.
        18. נדרש פירוט לגבי תמיכת המערכת באיתור התקני קצה (כגון IOT) בעלי פוטנציאל לסיכון (Rough Device).
        19. נדרש פירוט לגבי תמיכת המערכת בזיהוי והצגת פערי תצורה בנקודות הקצה כגון מערכת הפעלה ואפליקציות שאינן מעודכנות (Unpatched), הגדרות מערכת שגויות (misconfigurations), פערי אבטחה, שימוש בשירותים פגיעים, יציאות פתוחות וכדומה.
        20. נדרש פירוט לגבי תמיכת המערכת בביצוע בדיקות תאימות לנקודות הקצה אל מול הגדרות והקשחות מומלצות (Best Practice) של יצרן מערכת ההפעלה.
        21. נדרש פירוט לגבי תמיכת המערכת בביצוע בדיקות תאימות מערכת ה-XDR אל מול הגדרות והקשחות מומלצות (Best Practice) של יצרן מערכת ה-XDR.
        22. נדרש פירוט לגבי תמיכת המערכת בניטור שלמות קבצים (File Integrity Monitoring) על ידי סריקה והתראה בזמן אמת על שינויים חשודים שבוצעו בקבצים.
        23. נדרש פירוט לגבי תמיכת המערכת בביצוע בדיקת תאימות לנקודות הקצה בסביבת המזמין לאיתור איומים ופערי אבטחה אל מול תקנים ומסגרות אבטחת מידע בינלאומיים כגוןMITRE ATT&CK . נדרש פירוט לגבי כלל סוגי התקנים ומסגרות האבטחה הנתמכים במערכת.
        24. נדרש פירוט לגבי תמיכת המערכת בזיהוי דפוסים של נוזקות מאותה משפחה באמצעות יכולתGenetic malware detection .
        25. נדרש פירוט לגבי תמיכת המערכת בביצוע סריקות בזמן אמת להבטחה כי אין שימוש חריג בתעבורת התקשורת אל סביבת הלקוח וממנה.
     2. **יכולות הגנה ותגובה**
        1. על המערכת לכלול יכולות הגנה בזמן אמת בפני פעילות חשודה ו/או זדונית מתוחכמת ואיומים מתקדמים על נקודות הקצה לרבות התקפות מוכרות/לא מוכרות (Known/unknown Threats ,Malware ,Exploits, Ransomware, Zero-Day וכדומה). נדרש פירוט לגבי אופן המענה לדרישה זאת.
        2. על המערכת לכלול יכולת תגובה אוטומטית (Automated Response) לאיומים שזוהו על מנת להכיל אותם ולמנוע את התפשטותם בתוך הרשת, כגון בידוד מערכות מושפעות, חסימת כתובות IP זדוניות, הפסקת תהליכים זדוניים או מחיקת קבצים זדוניים.
        3. על המערכת לכלול יכולות הגנה המבוססת על טכנולוגיות AI/ML ( Supervisedו- unsupervised) לטובת לימוד התנהגותי של נקודות הקצה, זיהוי וניתוח אינטגרטיבי של מקורות מידע, תעבורת תקשורת, אירועים חריגים ודפוסי התנהגות המצביעים על פעילות זדונית ועל איום לסביבת הלקוח. נדרש פירוט לגבי אופן המענה לדרישה זאת.
        4. על המערכת לכלול יכולת בידוד (Isolate) או ניתוק נקודת קצה חשודה מהרשת, ולאפשר אליה גישה באמצעות המערכת לטובת חקירה.
        5. המערכת נדרשת להגן על דפדפנים בפני ניצול חולשות מהרחבות דפדפן ומאתרי אינטרנט זדוניים וגניבת זהויות (Credential theft). נדרש פירוט לגבי אופן המענה לדרישה זאת.
        6. נדרש פירוט לגבי תמיכת המערכת בהגנה על עותקי גיבוי של Shadow Copy ויכולת שחזור תחנה או קבצים לאחור בעקבות שינויים לא מורשים ופעילות זדונית שבוצעו בתחנה. (לדוגמה, במקרה של תחנת קצה בה הסוכן מופעל במצב Detect והיא הוצפנה על ידי Ransomware).
        7. נדרש פירוט לגבי תמיכת המערכת בהגנה בזמן אמת על זהויות משתמשים (Identity Protection) בסביבת Active Directory למניעת התקפות מבוססות זהות (כגוןPhishing , Password Attacks Credential Stuffing וכדומה).
        8. נדרש פירוט לגבי תמיכת המערכת ביכולת זיהוי וסיכול זמן השהייה של תוקף ברשת (dwell time).
        9. נדרש פירוט לגבי תמיכת המערכת בהגנה על נקודות קצה שאינן מחוברות לרשת האינטרנט (Standalone/Offline) או בעלות תקשורת אינטרנט מוגבלת.
     3. **חוקי מדיניות ואכיפה**
        1. על המערכת לכלול יכולות חומת אש בנקודות הקצה (Host Firewall) כגון יצירת חוקים ותנאי מדיניות מותאמים אישית לביצוע אכיפת תאימות ובקרת אבטחה בנקודות הקצה. במצב בו אינן מצייתות, נקודות הקצה תוצגנה כלא תואמות (noncompliant) ויהיה ניתן להחיל עליהן מדיניות מגבילה.
        2. על המערכת לכלול יכולת יצירת כללי FW כדי לאפשר או לחסום תעבורת רשת לנקודות הקצה בהתבסס על מידע חיבור, כגון כתובות IP, יציאות פורט, פרוטוקולים וכדומה.
        3. על המערכת לכלול יכולת יצירת Baseline אשר חריגות ממנו יוגדרו כאירועים חשודים.
        4. על המערכת לכלול יכולת בקרת התקנים (Device Control) בתחנות ושרתים. נדרש פירוט לגבי אופן המענה לדרישה זאת.
        5. נדרש פירוט לגבי תמיכה בניהול חוקי מדיניות מוגדרים מראש ומבוססי התנהגות (לדוגמה: מניעת התחברות לרשת הארגונית מנקודות חמות במקומות ציבוריים וכדומה).
        6. נדרש פירוט לגבי תמיכה ביכולות בקרת יישומים מורשים ((Application Whitelisting ואכיפה בזמן אמת של קבצי הרצה והגדרות בנקודות הקצה על בסיס פרמטרים מוגדרים כגון נתיב קובץ, SHA256 וכדומה.
        7. נדרש פירוט לגבי תמיכה ביכולות הצפנת דיסק (Disk Encryption) / יכולות ניהול הצפנת דיסק עבור Microsoft BitLocker בתחנות ושרתים.
        8. נדרש פירוט לגבי תמיכת המערכת ביצירת פרופיל פעילות משתמש לזיהוי תנועת איומים רוחבית (Lateral Movement) ומניעת התקפות מבוססת זהויות ((Identity-based attack.
     4. **יכולות ניהול נכסים ומשאבים**
        1. על המערכת לכלול יכולת מרכזית לניהול מלאי (Inventory) של נקודות הקצה בסביבת המזמין, לרבות שמירה על עדכניות מלאי של כל הנכסים והתוכנות בסביבה, כולל מפרטי חומרה, גרסאות תוכנה ותיקונים מותקנים. נדרש פירוט לגבי אופן המענה לדרישה זאת.
        2. נדרש פירוט לגבי יכולות המערכת לגילוי אוטומטי (Auto-Discovery) של נקודות הקצה בסביבת המזמין בארגון ובענן.
        3. נדרש פירוט לגבי תמיכת המערכת במנגנון סימון ותיוג (Tag) אוטומטי של נקודות על סמך קריטריונים מוגדרים מראש, וכן יכולת הוספה ידנית שאיננה חלק מתהליך הגילוי האוטומטי.
        4. נדרש פירוט לגבי יכולות המערכת לבצע חלוקות של כלל הנכסים והמשתמשים במערכת לתת קבוצות לפי פרמטרים שונים (כדוגמת טווחי IP, קונבנציית שמות, מע"ה, דומיין, אפליקציות, שירותים, תחנות חשודות וכו').
     5. **ניהול מרכזי, הצגת מידע ודו"חות**
        1. ממשק ניהול המערכת נדרש להציג תמונת מצב מרכזית מכלל רכיבי הקצה המנוטרים ולמקד את תשומת הלב באירועים וסיכונים החורגים מהנורמה.
        2. על המערכת לכלול יכולת הצגה אינטגרטיבית לכדי תמונת מצב אבטחתית ואחודה של פגיעויות, חולשות, חשיפות, איומים וסיכונים שאותרו בכלל נקודות הקצה בארגון לכדי ציון סיכון (Risk Score) משוכלל תוך שימוש בפורמטים מקובלים (כדוגמת CVSS). נדרש פירוט לגבי אופן המענה לדרישה זאת.
        3. המערכת נדרשת להתריע בפני מנהלי המערכת על אירועים חריגים שהוגדרו מראש, נדרש פירוט לגבי מנגנוני ההתרעה הקיימים בפתרון המוצע (מייל, SMS, התראה קולית, פלטפורמות העברת מסרים מידיים, התראה במערכת עצמה וכו').
        4. על המערכת לכלול יכולת יצירת מסכי תצוגה ומחוונים אינפורמטיביים על תהליכים בממשק הניהול המרכזי, לדוגמה הצגת כמות נקודות קצה, כמות משתמשים, אירועי אבטחה וכד'. יש לפרט את יכולות המערכת בביצוע התאמה אישית של המסכים.
        5. המערכת נדרשת לספק רשימה של נכסים, שירותים, משאבים, אובייקטים, משתמשים וכדומה אשר אינם עומדים במדיניות הארגון.
        6. על המערכת לאפשר הצגת התראות בתוך ממשק המערכת. יש לפרט את יכולות המערכת, הן לעניין סוגי ההתראות והן לגבי אופן הצגתן.
        7. המערכת נדרשת לתמוך ביכולת חיפוש באופן טקסטואלי, ופילטור לפי שדות, שמות מחשב, תאריכים, מערכות הפעלה, כתובות IP, פורטים, משתמשים, התראות וכדומה.
        8. על המערכת לכלול יכולת להנפקת דו"חות תקופתיים מוכנים ומותאמים אישית (כגון דו"ח סטטוס איומים ופעילות זדונית). נדרש פירוט לגבי סוגי דו"חות קיימים ללא עבודה נוספת מאת המשתמש וכן לגבי פורמטים נתמכים כדוגמת PDF, HTML ו-CSV.
        9. על המערכת לכלול יכולת ליצירת דו"חות שונים ומותאמים אישית, בהתאם לנכסים, שדות ו-Tags רלוונטיים. נדרש פירוט ודוגמא לדו"ח מערכת (כגון דו"ח סיכום פעילות חודשי, דוח פעילות משתמשים, דוח פעילות חשודה וכדומה) הכולל תקציר מנהלים, פירוט ממצאים והמלצות ליישום.
        10. נדרש פירוט לגבי תמיכה ביצירת דוחות תאימות (Compliance) המציגים את עמידת הארגון ביחס לבקרות ותקני אבטחה מקובלים.
     6. **ניתוח וחקירת אירועים חשודים**
        1. על המערכת לכלול ממשק ידידותי לניהול אירועים, חקירה ותגובה לאיומים ולתמוך הן בתהליכי חקירה ותגובה ידניים והן אוטומטיים. נדרש פירוט לגבי אופן המענה לדרישה זאת.
        2. המערכת נדרשת לאגור לוגים וראיות (Evidence) של כל אירוע בודד במערכת ובנקודות הקצה בעבור הצגה ומחקר מאוחר. נדרש פירוט לגבי משך הזמן בו נאגר המידע לאחור (retention) במערכת ובנקודות הקצה, וכן יכולת הלקוח לקביעת משך הזמן לשמירת המידע.
        3. על המערכת לכלול יכולות איסוף נתונים ממספר מקורות (Cross-Platform) כולל רשתות, נקודות קצה, FW, סביבות ענן ומערכות דואר אלקטרוני לטובת זיהוי וניתוח איומים ואירועי אבטחה (לדוגמה מידע על תהליכים וקבצים, שינויים בקבצי מערכת ו-Registry, חיבורי רשת, פעילות בין תהליכים, פקודות שורה, מטא-דאטה, קריאות DNS וכדומה). נדרש פירוט לגבי סוגי המידע ואופן המענה.
        4. על המערכת לכלול יכולת ניתוח ונורמליזציה של נתונים באופן אוטומטי לכדי תמונת מצב אירועים עבור כל זיהוי/מניעה המתרחשים. ניתוח זה יכלול בין היתר פירוט, נקודת כניסה (Entry point), כתובות IP, כתובות URL, מוניטין, מיקום גאוגרפי, עצי תהליכים ותיעוד השתלשלות האירוע ושרשרת התקיפה על פני ציר זמן.
        5. המערכת נדרשת לזהות ולהתריע בזמן אמת על פעילות חשודה, לתת ציון/דירוג בהתאם לרמת החשד, להתריע לאנליסטים ומנהלי המערכת ולספק המלצות ודרכי פעולה ישימות לתגובה ותיקון Remediation)).
        6. על המערכת לכלול יכולת לניתוח תקשורת על בסיס נתוני עבר ועל ידי מידע המצטבר עם הזמן מנקודות הקצה המנוטרות.
        7. על המערכת לכלול יכולת הצגה דינאמית וגרפית לניתוח אירועים כגון: מפת קשרים גרפית המציגה קשרים בין נכסים ואיומים חשודים, ניתוח פעילות חשודה על פני ציר זמן (timeline), נקודות כניסה (Entry points), ניתוח נתיב התקפה (Attack path analysis), ניתוח גורמי שורש (Root cause analysis) טופולוגית רשת, נזק פוטנציאלי וכדומה. נדרש פירוט לגבי אופן המענה.
        8. על המערכת לכלול יכולת ליצירת דו"ח חקר איומים המבוסס על מסגרת MITRE ATT&CK.
        9. על המערכת לכלול יכולת חיפוש בצורה פשוטה באופן טקסטואלי ופילטור לפי שמות, קבצים, שירותים, חולשות אבטחה, מזהים וכדומה בנקודות הקצה המנוטרות.
        10. נדרש פירוט לגבי כלל יכולות המערכת לתגובה לאירועים (Incident Response) הקיימות במוצר המוצע לרבות יכולות תיקון ומניעה ידניות ואוטומטית (Auto-remediation).
        11. נדרש פירוט לגבי יכולות חקר איומים חוצי-סביבות (Cross-domains).
        12. נדרש פירוט לגבי תמיכה בהקלטת session-ים, אחסונם, ניתוח שלהם והצגה חוזרת של אותם session-ים (כגון סיכום על גבי ציר זמן, סיכום טקסטואלי, צילומי מסך, סרט וידאו).
        13. נדרש פירוט לפי אילו פרמטרים ניתן להגדיר חריגה משגרה של פעילות רגילה כדוגמת שעות פעילות, ביצוע פעולות מיוחדות, חריגה משגרת פעילות של משתמש, כתובת IP חשודה, פורטים חשודים, פקודות ייחודיות, גישה ממיקום גאוגרפי וכו'.
        14. נדרש פירוט לגבי תמיכת המערכת ביכולות ציד איומים (Threat Hunting) על ידי חיפוש יזום דרך המערכת כדי לזהות איומים מתקדמים שטרם זוהו.
        15. נדרש פירוט לגבי תמיכה ביכולת חיפוש באמצעות שאילתות (Queries) וחוקי Yara לטובת ניתוח והצלבת נתונים ממספר מקורות מידע שונים במערכת.
        16. נדרש פירוט בנוגע לתמיכה המערכת בבנייה והחלת Playbooks וביכולות סימולציה לביצוע בדיקות טרום הרצה.
     7. **מודיעין איומי סייבר Cyber Threat Intelligence))**
        1. על המערכת לכלול יכולות מודיעין איומים מתקדמות המאפשרות איתור וניתוח איומי אבטחה כדי לשפר את יכולות הזיהוי והתגובה שלה. נדרש פירוט לגבי אופן המענה לדרישה זאת.
        2. המערכת נדרשת לספק מידע מפורט על אופי ומאפייני האיומים, לרבות וקטור התקיפה, Payloads, ומזהים (IOCs).
        3. על המערכת לכלול יכולת בחיבור למקורות מודיעין איומי סייבר. יש לציין את סוגי המקורות הקיימים במערכת ובכמה מקורות מודיעין המערכת תומכת בו-זמנית.
        4. על המערכת לכלול יכולת ניתוח והצגת חולשות ואיומים בזמן אמת/קרוב לזמן אמת אל מול מספר מקורות מודיעין סייבר שונים.
        5. נדרש פירוט לגבי תמיכה בהוספת מקורות (Feeds) מודיעין סייבר באופן ידני.
        6. נדרש פירוט לגבי תמיכה בהעשרת המערכת במזהים (IOCs) באופן ידני וממוכן .
        7. נדרש פירוט לגבי היכולת לשמור על IOCs שהוזנו על ידי המזמין באופן פרטי בסביבת המזמין וללא שיתופם לרשת הגלובלית של היצרן.
        8. נדרש פירוט לגבי תמיכה בשליטה והגבלה של שיתוף טלמטריה (לרבות IOC ו- Hashים) מסביבת המזמין לרשת הגלובלית של היצרן.
        9. נדרש פירוט לגבי תמיכת המערכת ביכולות ניתוח מודיעין מבוסס הקשר (Contextual Intelligence) המספק מדדי סיכון והתראה מפני פגיעה בנכסי הארגון על בסיס שילוב ניתוח איומים חיצוניים והערכת סיכונים פנימית.
        10. נדרש פירוט לגבי תמיכה ביכולת שיתוף מודיעין איומים עם ארגונים אחרים או פלטפורמות לשיתוף מידע מודיעין.
        11. נדרש פירוט לגבי שימוש המערכת ביכולת AI ולמידת מכונה כדי לחזות איומים עתידיים (Predictive Intelligence) על סמך נתוני מודיעין האיומים הנוכחיים.
        12. נדרש פירוט לגבי תמיכת המערכת ביכולות ציד איומים אוטומטי (Automated Threat Hunting) תוך שימוש בנתוני מודיעין האיומים לחיפוש יזום אחר אינדיקטורים לאיומים ברשת ובמערכות הארגון.
     8. **יכולת הפצה ועדכונים**
        1. על המערכת להתעדכן באופן תקופתי ושוטף הכולל בין היתר עדכוני תוכנה קבועים, עדכוני מערכת, עדכוני אבטחת מידע, תיקון באגים/פגיעויות/חולשות/חשיפות שאותרו ועוד, וזאת בהתאם להגדרות היצרן. נדרש פירוט לגבי מדיניות היצרן בנושא.
        2. על המערכת לכלול יכולת מרכזית של הפצה/התקנה/הסרה/עדכון סוכן המערכת בנקודות הקצה (Endpoints) באופן אוטומטי תחת תיחום ומדיניות מוגדרת, ובאופן ידני (כגון תמיכה בסקריפטים).
        3. כלל העדכונים המופצים לסוכן המערכת נדרשים להיות חתומים על ידי היצרן.
        4. על המערכת לכלול יכולת מרכזית לביצוע בדיקת סטטוס עדכני של גרסאות סוכנים, עדכוני תוכנה ועדכוני אבטחה בנקודות הקצה.
        5. נדרשת תמיכה ביכולות proxy לעדכון נקודות הקצה ברשתות שאינן מחוברות לרשת האינטרנט (Offline), או בעלות תקשורת מוגבלת. נדרש פירוט לגבי אופן המענה.
        6. נדרש פירוט לגבי שיטות ההפצה הנתמכות על ידי המערכת כגון הורדה באמצעות לינק ישיר מפורטל, וכן תמיכה בכלי הפצה כגוןGPO ,SCCM וכדומה.
        7. נדרש פירוט לגבי אופן ביצוע העדכון כאשר תחנה נמצאת מחוץ לרשת המשרד.
        8. נדרש פירוט לגבי אופן ביצוע התקנה ועדכון לתחנות מבודדות (Standalone).
        9. נדרש פירוט לגבי תמיכה בשדרוג גרסאות סוכן מבלי לבצע אתחול (reboot) לעמדת הקצה.
     9. **ממשקים עם מוצרי צד ג'**
        1. על המערכת לכלול תמיכה בממשק למול מערכות ניטור אבטחתי ואוטומציה כגון SIEM ו- SOAR. נדרש פירוט לגבי אופן המענה.
        2. על המערכת לכלול תמיכה בספקי שירות לניהול זהויות (IdPs). נדרש פירוט לגבי אופן המענה.
        3. נדרש פירוט לגבי אפשרויות האינטגרציה הקיימות במערכת, כגון RESTful APIs, ערכות פיתוח תוכנה (SDK) ואינטגרציות מובנות מראש.
        4. נדרש פירוט לגבי תמיכת המערכת באינטגרציה למוצרים נוספים של ספקי צד ג' (כגון מוצרי אבטחת מידע ותקשורת, שירותי מייל, שירותי הזדהות, שירותי ענן, כלי אוטומציה, כלי ITSM, כלי Ticketing, וכדומה).
        5. נדרש פירוט לגבי תמיכת המערכת בהצעת יישומים וממשקים לאפליקציות מתוך Marketplace של היצרן.
  3. **מפת דרכים**
     1. נדרש פירוט לגבי מפת הדרכים של היצרן בתחום התיחור, תוך התמקדות בתכונות מרכזיות (Main Features) וכן לוחות זמנים לשנה הקרובה.
  4. **תשתית המערכת**
     1. השירות יופעל על גבי פלטפורמת הענן הציבורי עליה מבוסס השירות המוצע, וזאת בהתאם לכללים המפורטים להלן:
        1. השירות נדרש לפעול מאזור ענן ציבורי (Region) של אחד מספקי הענן – Amazon Web Services ו-Google GCP בשטח הטריטוריאלי של מדינת ישראל (להלן: "**האזור הישראלי**"), או לחילופין, על בסיס האזור הגדול ביותר שמופעל על ידי היצרן בתחומי האיחוד האירופי (להלן: "**אזור חו"ל**"). ככלל, כל הנתונים הפרטיים (Personal Identifiable Information – כהגדרתם בתקנות ה-GDPR כגון: שמות משתמש, כתובות דוא"ל, שמות מלאים, מספרי טלפון, כתובות, תיאורי תפקידים, תמונת פרופיל) של המשתמשים יהיו מאוחסנים ומעובדים אך ורק בתוך האזור (Region) הספציפי שממנו הוגדר מתן השירות עבור המזמין. נדרש פירוט לגבי אופן המענה לדרישה ולגבי חריגים נדרשים לתפעול המערכת, ככל וישנם.
        2. ככל הניתן, מידע מערכתי כגון Metadata, מידע תפעולי, טלמטריה, ואינדיקציה לאירוע אבטחה יעובד ויאוכסן בתוך האזור הספציפי שהוגדר עבור המזמין. על המציע לפרט את המידע היוצא מגבולות האיזור, את אמצעי ההגנה עליו ואת המורשים לגשת אליו.
     2. יש לפרט את תצורת המערכת לרבות התייחסות לנושאים הבאים:
        1. תשתיות הענן הציבורי עליהם הפתרון מבוסס, מבין פלטפורמות ספקי הענן.
        2. מיקום גאוגרפי של האזור (Region) הספציפי ממנו יינתן השירות המוצע.
        3. האם החשבון עליו פועלת המערכת הינו ייעודי למערכת המוצעת או שהינו משותף לכלל המזמינים.
     3. **תצורת עבודת המערכת המוצעת**
        1. יש לפרט את תצורת פעולת המערכת המוצעת תוך התייחסות לנקודות הבאות:
           1. מיקום ואופן שמירת מידע מוגן – ב-"רשת" (כגון VPC) של המזמין, אצל הספק, אצל היצרן או בכל מקום אחר. ככל והמידע אינו נשמר אצל המזמין יש לפרט את המידע ומיקום שמירתו.
           2. מיקום עיבוד נתוני תוכן (כהגדרת המונח להלן) – ב-"רשת" (כגון VPC) של המזמין, אצל הספק, אצל היצרן או בכל מקום אחר. ככל ונתוני התוכן אינם מעובדים אצל המזמין יש לפרט את סוג המידע ומיקום שמירתו.
           3. ככל ששמירת החומר והעיבוד הינה באזור ייעודי שהוגדר עבור המזמין (כגון Bucket ייעודי לשמירת הלוגים שמגיעים מהסוכנים), יש לפרט את יכולת הגישה או השליטה של הספק או היצרן על המידע או רכיבי המערכת ככל וישנה.
        2. יש לפרט את תצורת קישור המערכת לרשת המזמין תוך התייחסות לנקודות הבאות:
           1. אופן קישור רשת המזמין בענן (כגון VPC), יש לפרט האם הקישור הינו לדוגמה בתצורת VPC Endpoint, Peering, Private Link, או שהשירות מיוצג ברשת המזמין עצמה, או דרך קישור VPN או באופן אחר, מה אופן אבטחת הקישור והאם נדרשת פתיחת כתובות חיצוניות לצורך קישור לשירות.
           2. הממשק למערכת הניהול של השירות, יש לפרט האם הקישור הינו לדוגמה בתצורת VPC Endpoint, Peering,Private Link , או שהשירות מיוצג ברשת המזמין עצמה, או דרך קישור VPN או באופן אחר, מה אופן אבטחת הקישור והאם נדרשת פתיחת כתובות חיצוניות לצורך קישור לשירות.
     4. **ההון האנושי**
        1. יש לפרט את תהליכי הבקרה, האימות והסינון המתבצעים לעובדי היצרן וספקי המשנה תוך התייחסות להבדלים בתהליכים בהתאם לסוגי העובדים ורמות הסיכון הגלומות בתפקידם.
        2. יש לפרט את תהליכי ההכשרה והריענון לנהלי האבטחה, הביטחון והסייבר לעובדי היצרן ולספקי המשנה.
        3. יש לפרט את תהליכי ההכשרה וההסמכה המקצועית של אנשי המקצוע של היצרן ושל ספקי המשנה.
        4. יש לפרט את מנגנוני הפיקוח על קיום הנהלים ואופן הטיפול בהפרות נהלי אבטחה או נהלים קריטיים אחרים.
        5. יש לפרט האם מופעלים כלים לאיתור סיכוני אנוש (כגון איתור חריגות התנהגותיות, משובי מנהלים או עמיתים על בעיות וכו') של בעלי תפקידים רגישים או בעלי הרשאות גישה גבוהות.
     5. **אבטחת שרשרת האספקה**
        1. יש לפרט את התקן לפיו מאובטחת שרשרת האספקה, כגון NIST SP 800-53 Rev. 5/Nist SP 800-161 Rev. 1, ISO 28000, תקן בינ"ל אחר, או לצרף את הנוהל הפנימי, ככל שיש.
        2. יש לפרט את אמצעי האבטחה על שרשרת האספקה לרבות הנושאים הבאים:
           1. תהליכי הבקרה על הכנסת תוכנה ממקור חיצוני והעדכונים לה, לרבות איתור חולשות, backdoors או הטמנות עם יכולות פוגעניות.
           2. תהליכי הבקרה על הכנסת תוכנה ממקור פנימי והעדכונים לה, לרבות איתור חולשות, backdoors או הטמנות עם יכולות פוגעניות.
           3. יש לפרט כל תהליך או בקרה רלוונטיים נוספים.
        3. יש לפרט את תהליך הפיקוח והבקרה על הספקים החיצוניים לרבות התקנים לפיהם הבקרה מתבצעת.
     6. **המידע הנאגר אצל היצרן**
        1. יש לפרט את המידע הנאגר אצל היצרן במהלך מתן השירותים, כגון נתוני עיבוד (כהגדרת המונח להלן) או נתוני גישה (כהגדרת המונח להלן).
        2. יש לפרט את מדיניות מחיקת המידע (Retention policy) וכן את המנגנונים המשמשים אותו למחיקת המידע כאשר הדבר נדרש.
        3. ככל שנשמרים נתונים אצל הספק או היצרן, יש לפרט את אמצעי ההגנה על המידע ואת הכלים והתהליכים הבאים על מנת למנוע גישה בלתי מורשית למידע.
        4. יש לפרט את תהליך מתן הגישה לנתונים אלו ואת קבוצות המשתמשים הרשאים לצפות במידע ואת תהליכי הבקרה לאיתור שימוש לרעה בהרשאות אלו.
     7. **אבטחת תצורה וניהול שינויים**
        1. על היצרן לפעול על פי מדיניות מסודרת לניהול תצורה ושינויים של כלל המערכות השותפות במתן השירותים, בהתאם לתקנים המקובלים והנדרשים.
        2. יש לפרט את התקן על פיו מבוצעים תהליכים אלו, ככל שישנו, תוך תיאור עקרוני של מערכות בקרת התצורה ותהליך בקרה, אישור ותיעוד השינויים.
        3. יש לפרט בקרות למניעת Downgrade לא מאושר של מנגנוני הצפנה, מנגנוני ניהול מפתחות, מערכות הגנה או שירותי הגנה ככל וישנם.
        4. יש לפרט את אופן ההגנה והבקרה בתהליכי הפיתוח, כגון תהליך פיתוח מאובטח SDLC)) ותקנים רלוונטיים ככל והיצרן עומד בהם.
     8. **הגבלת גישת תמיכה**
        1. יש לפרט את תהליך התמיכה במערכת, מי הגורמים התומכים, האם מדובר בגורמים מטעם הספק, היצרן או ספק הענן ואת התהליך המיושם אצל הספק והיצרן במקרה של צורך בגישה כאמור, לרבות מסלולי אישורים פנימיים, תהליכי האישור מול המזמין, אבטחת הגישה, אופן תיעודה (לרבות רישום לוג, הקלטות Session) וכו'.
        2. יש לפרט האם ניתן ליישם מנגנון בו כל גישת תמיכה לרכיבים המשמשים את המזמין והמכילים או המאפשרים גישה לנתוני עיבוד תתבצע רק לאחר יישום תהליך אישור מוגדר אשר במסגרתו יהיה צורך לקבל את אישור נציג המזמין עבור גישת התמיכה.
     9. **ניהול סיכונים**
        1. אם קיים אצל היצרן מנהל אבטחת מידע האחראי על אבטחת המידע בשירותים המוצעים, יש לפרט את תיאור תפקידו והאם הינו חבר הנהלת היצרן.
        2. יש לפרט את תהליכי ניהול הסיכונים אצל היצרן.
        3. יש לפרט את הגורמים המבצעים תהליכים אלו, את דרגי הפיקוח, דרגי האסקלציה לטיפול בסוגיות ואופן הטיפול בממצאים שלא טופלו.
        4. יש לפרט את הכלים, האמצעים ואופן מימושם על מנת לאפשר ניהול הסיכון באופן דינאמי ובהתאם לשינויים במתאר האיומים ובשירותים המסופקים.
     10. **הזדהות עבור השירות המוצע**
         1. על השירות לתמוך בפרוטוקולי הזדהות סטנדרטיים כגון SAML, OpenID, OAuth לצורך ביצוע Single Sign On עם מערכות המזמין וכן תמיכה ביכולת Multi Factor Authentication. יש לפרט את פרוטוקולי ההזדהות הנתמכים (כגון U2F, FIDO, OTP).
         2. יש לפרט את יכולת ההתממשקות עם כלי IAM למערכות ניהול משתמשים ולמערכות צד ג' לניהול זהויות.
         3. יש לפרט את התמיכה במתן גישה באופן פרטני ברמת תפקידים RBAC – Role Based Access Control, וברמת תכונות ABAC – Attribute Based Access Control.
         4. על השירות לתמוך בקבלת פרטי המשתמשים ממערכת הזדהות מרכזית בפרוטוקולים סטנדרטיים.
     11. **שרידות והמשכיות עסקית (SLA) של השירות המוצע**
         1. נדרש פירוט לגבי נתוני הזמינות (Uptime) בהם מתחייב לעמוד היצרן.
         2. יש לפרט את המנגנונים המבטיחים את שרידות השירות והמידע לרבות פריסת המערכת בין מתחמים שונים, אופן גיבוי המידע, שמירה על שלמות הגיבוי, בדיקת יכולת השחזור, עמידה בתרחישי כשל שונים וכו'.
         3. אם מבוצעים גיבויים מחוץ לסביבת הענן, יש לפרט את המנגנון המוודא את השמדת מצע זיכרון ורכיבים שסיימו שירות (כגון, הוצאתם מהמערכת, החלפתם או במקרה של תקלה).
         4. יש לפרט את אופן הבקרה של היצרן על איכות השירות הניתן מהאזור הענן הציבורי ואת רמות האסקלציה המוגדרות בנהליו.
         5. נדרש כי ניתן יהיה לגבות או לייצא את **נתוני המערכת** למצע שבשליטת המזמין באופן שוטף. יש לפרט את פורמט הגיבוי ותאימותו למערכות סטנדרטיות בשוק.
     12. **הגנת תשתיות השירות אצל היצרן**
         1. היצרן נדרש להפעיל SOC אשר מנטר מערכותיו בהיבטי סייבר 7/24 (24 שעות ביממה, 365 ימים בשנה). יש לפרט את יכולות ה-SOC המופעל על ידי היצרן, מערכת ה-SIEM בה הוא עושה שימוש ורכיבים ויכולות נוספות המשמשים את ה-SOC בפעולתו השוטפת. אם השירות מופעל על ידי קבלן משנה של היצרן, יש לפרט בנוסף את פרטיו.
         2. יש לפרט שימוש באמצעי הגנה על נקודות קצה (EPP/EDR/XDR) בסביבת היצרן. אם קיים כשירות המופעל על ידי קבלן משנה של היצרן (MSSP), יש לפרט בנוסף את פרטיו.
         3. יש לפרט שימוש בכלי אוטומציה לניטור וטיפול באירועים. יש לפרט את מתודולוגיית הפעולה של היצרן (כגון SOAR), הכלים הרלוונטיים ואופן מימושם.
         4. התעבורה הנכנסת והיוצאת לתשתית השירות תנוטר לאיתור תקיפות או פעילות חשודה. יש לפרט את יכולות היצרן בתחום ותהליכי העבודה המיושמים על ידו לצורך כך.
         5. היצרן מיישם תהליכי ניטור ותהליכי עבודה בתצורת Privacy by Design תוך חשיפה מינימלית של מידע לגורם אנוש. יש לפרט את הכלים והמתודות אשר היצרן מיישם לצורך מימוש תהליכים אלו.
         6. אם היצרן מבצע שימוש בכלים לניטור רציף של משטח חשיפה של התשתית (Attack Surface Management), יש לפרט את כל הכלים ותהליכי העבודה בהם נעשה שימוש.
         7. יש לפרט את האמצעים המופעלים לצורך הגנת המערכות המשמשות למתן השירותים מפני שינויים בלתי מורשים ואת אמצעי הניטור המופעלים על ידי היצרן לצורך בקרה על כך.
         8. כלל התשתיות, המערכות והשירותים המוצעים מעודכנים בכלל עדכוני האבטחה הרלוונטיים על ידי היצרן. יש לפרט את תהליכי העדכון ותדירות ביצוע העדכונים.
         9. כלל המשתמשים אשר יכולים לגשת למידע של המזמינים או בעלי הרשאות גישה גבוהות (Privileged Access) כגון: Administrators, Operators, Support, DevOps וכו,' ינוטרו ויזדהו ברמה גבוהה. יש לפרט את תהליכי העבודה והכלים המיושמים לצורך כך.
         10. יש לפרט את אופן ההגנה על נתוני הגישה של משתמשי המערכת, לרבות בקרת הגישה אליהם, הצפנתם, כלי האבטחה המגנים מפני גישה בלתי מורשית או דלף.
         11. יש לפרט את אופן ההגנה על ממשקי ניהול המערכת, הפרדה בין משתמשים, מניעת גישת גורמים בלתי מורשים, לרבות עובדי הספק, עובדי היצרן או קבלני המשנה שלו.
         12. יש לפרט את אופן ההגנה על ממשקי API של המערכת, פנימיים וחיצוניים.
     13. **כלי אבטחה המשמשים להגנת השירותים המוצעים**
         1. יש לפרט על כלי ניתוח מתקדמים, אוטומטיים, לרבות משולבי יכולות AI, לאיתור פעילות חשודה בשירותי המשתמשים, ניסיונות לחשיפה או חשיפה של מידע רגיש, וכו'.
         2. יש לפרט כלי בקרה, ניטור והגנה בסייבר נוספים בהם עושה היצרן שימוש, ואשר יכולים לשמש את המזמינים על מנת לשפר את ההגנה על המידע שברשותם, כגון יכולות DLP, התמודדות עם קוד זדוני וכו'.
     14. **הצפנה וניהול מפתחות בשירותים המוצעים**
         1. יש לפרט את יכולות ההצפנה של המידע בשכבות השירות השונות.
         2. כל נתוני המערכת יהיו מוצפנים במנוחה (at rest) ובתנועה in transit)), כברירת מחדל.
         3. יש לפרט את סוגי ואלגוריתמי ההצפנה המשמשים את היצרן בשירותיו כגון הצפנה במנוחה (at rest), הצפנה בתנועה (in transit), והצפנה בזמן עיבוד (runtime encryption), התקן עליהם הם מבוססים, ואסמכתאות חיצוניות לחוסן אלגוריתמי ופרוטוקולי ההצפנה.
         4. יש לפרט את אופן ניהול ושמירת המפתחות ביחס לכל אחת משכבות השירות וסוגי השירותים השונים.
         5. יש לפרט לגבי תמיכה בממשק לתשתיות ניהול מפתחות אליהן היצרן מתממשק (כגון KMS).
         6. אם היצרן מפעיל תשתית ניהול מפתחות עצמאית, יש לפרט לגבי הפתרון המוצע בדגש על עמידה באופן מלא בתקן FIPS- 140-2 level 2 ומעלה.
         7. יש לפרט את יכולות המערכת בעבודה בתצורת Bring Your Own Key לרבות יכולת ההגנה על המערכת, הקשחתה, ואת יכולת השליטה של המשתמש בפרמטרים השונים של מפתחות ההצפנה.
         8. כלל תהליכי חילול, שינוי, החלפה, ביטול מפתחות או כל פעולה אחרת בקשר עם מפתחות הצפנה, יבוצעו על ידי המזמין ללא כל יכולת צפייה או גישה של הספק או היצרן (מעבר למערכות החייבות גישה למפתח לצורך פעולת השירות) או כל גורם אחר שלא הותר על ידי המזמין.
     15. **איסוף לוגים וניטור**
         1. המזמין יוכל לקבל את כלל נתוני העיבוד והגישה למערכותיו תוך תמיכה בהעברת הנתונים למערכות SIEM של המזמין, עורך המכרז או של גורם שלישי. יש לפרט את אופן העברת הלוגים (ממשק Online, העברת קבצים עיתית, API וכו'), למערכות ה-SIEM הנתמכות (כגון Chronicle ו- QRadar) ואת היקף התמיכה.
         2. יש לפרט את מקורות הלוג האפשריים (כגון: תשתית, תשתית יישומית, יישום, א"מ וכו').
         3. יש לפרט את עדכניות המידע (הזמן מקרות האירוע עד העברת המידע), היקף המידע, יכולת החקר של המזמין או בא כוחו וכו'.
         4. יש לפרט את פרק הזמן בו נשמרים נתוני העיבוד ונתוני הגישה על ידי היצרן, את מדיניות היצרן בקשר לשמירת נתונים אלו ואופן הגנתם.
     16. **חקירה**
         1. יש לפרט את יכולות היצרן, הכלים ותהליכי העבודה שלו בתחום חקירה ותגובה לאירועי סייבר במערכות היצרן.
         2. יש לפרט את תהליך הפעלת מערכי ה-Incident Response, ככל וישנם, במקרה של צורך בחקירת אירוע אבטחה, מעורבות ספק הענן, זמני התגובה, המשאבים הנגישים למזמין, תצורת הממשק וכו'.
     17. **בקרה פנימית ועמידה בתקנים**
         1. על השירות לעמוד, לכל הפחות, באחד מהתקנים הבאים:
            1. תקן ISO27001 או תקן SOC 2 AICPA, יש לפרט את התקן בו השירות עומד.
            2. יש לפרט תקנים נוספים בהם השירות עומד כגון: ISO27017, ISO27018, CSA STAR level 2 וכו' אם קיימים.
         2. יש לפרט את תהליכי העבודה בארגון והמערכות/כלים בהן משתמש היצרן אשר מטרתם לוודא את עמידת השירות בכל הכללים והתקנים אשר הוא מחויב להם (Compliance).
         3. יש לפרט את דרגי הפיקוח, דרגי האסקלציה לטיפול באירועים, ואופן הטיפול בממצאים שלא טופלו.
     18. **הפרדה ומידור לקוחות (Tenants)**
         1. יש לפרט את יכולות היצרן, ככל שישנן, לבצע בידוד ובידול של Tenant (לקוח) זה או אחר, בהתייחס לנקודות הבאות:
            1. אופן ההפרדה והבידול של שירותים משותפים והאמצעים למניעת דלף מידע בין Tenants שונים, גישת משתמשי Tenant מסוים למשאבי Tenant אחר, הפרדת ניהול ובקרה וכו'.
            2. יכולת מניעה גישת משתמשי לקוח מסוים למשאבים של לקוח אחר (זר), למעט אם אושרה גישה כאמור, גם אם למשתמש הרשאות גישה למשאבי הלקוח הזר. יש לפרט את יכולות המניעה שאינן מבוססות מערכת ההזדהות.
            3. יכולת מניעה גישת משתמשי לקוח זר, למשאבי הלקוח, למעט אם אושרה גישה כאמור, גם אם למשתמש הזר הרשאות גישה למשאבי הלקוח. יש לפרט את יכולות המניעה שאינן מבוססות מערכת ההזדהות.
            4. יכולת יצירת כתובת (IP או URI) ייעודית ופרטית לשירות עבור משתמשי לקוח או קבוצת מזמינים, אשר אינה משותפת עם לקוחות אחרים.

5. נספח ד' – מודל הייחוס

* 1. כל המחירים יכללו אחריות כנדרש בפרק 3 למסמכי המכרז המרכזי וכמפורט לעיל במסמכי התיחור.
  2. על המציע להזין הצעתו, במחירי המחירון הרשמי, על גבי גיליון האקסל המצורף כנספח ד'1 להודעה על פרסום מסמך התיחור.
  3. המחירים ייקבעו בתיחור הדינאמי המקוון בהתאם למפורט לעיל.
  4. שירותי התקנה, הטמעה ותחזוקה

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **סעיף** | **כמות לשקלול** | **תעריף מקסימום (כולל מע"מ)** | **הערות** |
| א' | מחיר תחזוקה שנתית, באחוז ממחיר המוצר בפועל (מהשנה השנייה ואילך) | 4 | 20% | סה"כ חמש שנים לשקלול בתיחור. |

* 1. **הערות**
     1. כל מזמין יבצע רכש בפועל, בהתאם למס' המשתמשים הנדרש לו. אם מחירון היצרן כולל מחיר לרישוי בודד ולפי מדרגות מחיר בהתאם למס' המשתמשים להם נרכש רישוי, מחיר הרישוי לכל כמות משתמשים יהיה בהתאם למחירון הספק לרישוי בודד לפי מדרגה של 50,000 רישיונות או לפי היקף ההזמנה בפועל, בהתאם למחיר הרישיון הנמוך מביניהם. הכל, לאחר החלת ההנחה שתיקבע בתום התיחור. האמור תקף לכלל המוצרים והשירותים הניתנים לרכישה, גם לגבי כאלו שיתווספו לאורך תקופת ההתקשרות.
     2. אם מודל התמחור של המוצר הינו במינוי (**Subscription**) תחושב העלות לפי המודל הבא:
        1. מחיר המינוי לשנה יוכפל ב-5 – בהתאם לאופק החישוב בתיחור, המפורט לעיל. כלומר, סה"כ עלות הרכש והתחזוקה יתומחרו כראוי לתקופת השוואה בת 5 שנים.

**לדוגמא**, אם מחיר המינוי לשנה עבור רכיב מסוים הוא 100$, מחיר הפתיחה של סה"כ העלות ל-5 שנים עבור אותו רכיב יהיה 500$, כאשר עלות זו תכלול את כל עלויות הרכש והתחזוקה לתקופה זו.

* + - 1. לצורך התיחור הדינאמי, וככל שיהיה צורך לציין את מחיר התחזוקה, מחיר התחזוקה יקובע ל-20% ממחיר הרכישה ו**לא ישוקלל בחישוב עלות ההצעה**. לרכיב זה לא תהיה כל השפעה על המחיר או על אחוז ההנחה.
      2. ההנחה על מחיר המינוי השנתי שתיקבע בסוף התיחור תהיה תקפה לכל שנה שתירכש על ידי המזמין, גם לאחר השנה החמישית. מחיר זה יכלול את כל עלויות הרכש והתחזוקה, כאמור בסעיף ‎1.5.3.3 לעיל.

6. נספח ה' – הצהרת יצרן

**ניתן לחתום על הצהרה זו בעברית או באנגלית**

**הצהרת יצרן**

**לכבוד**

**מינהל הרכש הממשלתי, החשב הכללי משרד האוצר**

הנדון: תיחור מס' 4 לאספקת מערכות XDR – Extended Detection & Response ושירותים נלווים עבורן (להלן: "**התיחור**") המתפרסם במסגרת מכרז מרכזי 05-2022 לרכש ואספקת מוצרים ושירותים בתחום אבטחת המידע והגנה בסייבר עבור משרדי הממשלה ויחידות הסמך (להלן: "**התיחור**")

אני, הח"מ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, מחברת \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, בעלת הקניין הרוחני של המוצרים והשירותים המוצעים בתיחור (להלן: "**היצרן**") על ידי \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (להלן: "**המציע**"), מצהיר/ה בזה כדלקמן:

1. המציע, אשר מציע מוצרים ושירותים מתוצרתנו לתיחור, מוסמך ע"י היצרן למכור, להתקין ולתת שירות למוצרים ושירותים בתחום התיחור בישראל, כמורשה מטעם היצרן, לתקופה של לפחות 12 חודשים טרם המועד האחרון להגשת הצעות בתיחור.
2. המציע הינו (*יש לסמן את אחת האפשרויות)*:

ספק מורשה שלנו בישראל עבור המוצרים והשירותים המוצעים.

חברתנו (היצרן) או חברה-בת שלנו בישראל.

1. המציע מחזיק בהסמכה הגבוהה ביותר של היצרן בתחום התיחור והוא מורשה על ידי היצרן למכור את השירות ולהתחייב לדרישות המכרז והתיחור עבור השירות.
2. היצרן מאשר כי הוא מכיר את תנאי המכרז והתיחור.
3. היצרן מתחייב:
   1. כי למיטב ידיעתו אין כל מניעה כי המציע בתיחור יספק את המוצרים ו/או השירותים של היצרן בתנאים הנדרשים במכרז למשך כל תקופת התיחור, לרבות תקופות האופציה הכלולות בה.
   2. לתת את מלוא הגיבוי למציע בארץ, לספק ולהעמיד לרשות המציע במכרז את השירותים ו/או מוצרי היצרן על מנת שהוא יעמוד בתנאים הנדרשים במכרז, לוודא כי השירותים עומדים בדרישות המכרז והתיחור, לספק ולהעמיד כוח אדם מומחה ומיומן, להקים מנגנון אסקלציה מהספק אליו, ולסייע בשמירת הרציפות במתן האחריות למוצרים מתוצרתו, כל זאת למשך כל תקופת התיחור, לרבות תקופות האופציה הכלולות בה.
   3. תנאי השירות יהיו התנאים המפורטים במסמכי המכרז ובתיחור. בהיעדר הוראה מפורשת או משתמעת בהוראת ההסכם או המכרז יחול הסכם השירות (service agreement) הסטנדרטי והפומבי של היצרן אשר משמש באזור חו"ל עבור לקוחות בסדר גודל של ממשלת ישראל.
   4. השירות יופעל באזור הישראלי בהתאם להוראות סעיף ‎4.7.1 למסמכי התיחור, ובתצורה המקובלת של השירות באזורים אחרים בחו"ל בהם השירות פרוס.
   5. המענה לנספח ג' לתיחור נעשה באופן התואם את מאפייני השירות ואופן אספקתו על ידי היצרן.
   6. היצרן מתחייב כי כל דבר הנדרש מהמציע ואשר לצורך מימושו נדרש סיוע של היצרן, היצרן יספק את כלל הסיוע כאמור.
   7. היצרן יעשה את כל הנדרש ממנו על מנת שהמציע יעמוד בתנאי המכרז ובהסכם מכוחו הנדרשים מהיצרן לצורך אספקת השירות, לכל אורך תקופת ההתקשרות.
   8. במקרה בו יבצר מהמציע להמשיך לתת את השירותים, יהיה היצרן או נציגו מחויב לסייע במעבר לאספקת המוצרים והשירותים ע"י ספק חדש שיקבע עורך המכרז.
   9. לעדכן את המציע ועורך המכרז באופן מיידי בדבר פריטים אשר קיימת היתכנות להפסקת ייצורם, שיווקם או התמיכה בהם (END OF LIFE, END OF SALE או END OF SUPPORT) או שכבר הוכרזו ככאלה.
   10. שלא לפרסם את דבר הזכייה של המציע בתיחור מסוים ללא אישור מראש של עורך המכרז.

|  |
| --- |
| שם היצרן: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| תפקיד החותם אצל היצרן: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| תאריך: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  חתימה וחותמת: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Manufacturer's Declaration for a specific invitation

**To:**

**Israel Government Procurement Administration (IGPA), Accountant General, Ministry of Finance, Israel**

**Re**: **Specific invitation number 4 for the supply of** XDR – Extended Detection & Response **products and accompanying services published as part of Central Tender 05-2022 for the Procurement and Supply of Cyber Security Products and Services for the Government Ministries and Additional Government Units] (hereinafter: the "Specific Invitation")**

I the undersigned, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, of the company \_\_\_\_\_\_\_\_\_\_\_\_\_\_, which owns the intellectual property of the products and services offered in the Specific Invitation (hereinafter: the "**Manufacturer**") by the bidder \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (hereinafter: the "**Bidder**"), having been advised that I must tell the truth and that I will be subject to the penalties stipulated by law if I fail to do so, hereby declare that:

1. The Bidder, offering the products and services manufactured by us in the domain of the Specific Invitation, is currently authorized by us for the sale, supply, install and service of our products and services in Israel for at least the last twelve (12) months before the Specific Invitation submission deadline.
2. The Bidder is [check appropriate box]:

A licensed supplier/authorized reseller of the Manufacturer for the services and products offered.

The manufacturer or a subsidiary of the Manufacturer in Israel.

1. The Bidder is certified by us, the Manufacturer, at the highest certification level available for the offered product line, and holds the full rights to sell the service and to commit to the requirements of the Tender and the Specific Invitation.
2. The Manufacturer confirms it is familiar with the terms of the Tender and the Specific Invitation.
3. The Manufacturer undertakes a commitment to:
   1. That to the best of its knowledge, there is nothing to prevent the Bidder from supplying the products and/or services of the Manufacturer in accordance with the terms and conditions of the Tender for the entire duration of the Specific Invitation period, including the optional periods.
   2. Provide full support to the Bidder in Israel, to supply to the Bidder with products and services needed to fulfill the Tender, ensure that the services meet the requirements of the Tender and the Specific Invitation, and to provide support of skilled and experienced personnel and continuous Warranty for the products and services manufactured by it, and establishing an escalation process from the Bidder to it, for the entire Specific Invitation period, including the optional periods.
   3. The terms of the service will be the terms specified in the Tender and the Specific Invitation. In the absence of an explicit or implicit provision in the provisions of the agreement or the Tender, the standard and public service agreement of the Manufacturer which is used in the overseas region for customers of the size of the Israeli Government will apply.
   4. The service will be operated in the Israeli Region in accordance with the provisions of section ‎4.7.1 of the Specific Invitation documents, and in the accepted configuration of the service in other overseas regions where the service is deployed.
   5. The response to Appendix C ("ג") of the Specific invitation is made in a manner consistent with the characteristics of the service and the manner of its delivery by the Manufacturer.
   6. The Manufacturer undertakes that whatever is required from the Bidder plus the required assistance of the Manufacturer for the realization thereof, the Manufacturer will provide all the aforesaid assistance.
   7. Do all in its power to provide continuous warranty for the products and services manufactured by it, inter alia by cooperating with the transfer of sales and warranty for the products and/or services to another supplier which will be determined by the IGPA, including in the event that the Bidder or the Manufacturer will not be able to continue to supply the products and/or services.
   8. Immediately inform the Bidder and the IGPA about products and services which are at the end of production, sale or service and support cycle (End Of Life, End Of Sale or End Of Support).
   9. Not to publish any information regarding the Bidder's win with respect to any specific Invitation published as part of this Tender.

[All terms – as defined in the Tender]

|  |  |
| --- | --- |
| Name of Manufacturer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Position with Manufacturer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Signature and seal: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

7. נספח ו' – בקשה לחיסיון פרטים מתוך ההצעה

* 1. אם המציע סבור כי בהצעתו יש חלקים שהם בגדר סוד מסחרי או סוד מקצועי, עליו למלא את הטבלה להלן.
  2. מציע שטען שחלק מסוים מהצעתו הוא סוד מסחרי או מקצועי, או מכל טעם אחר המוזכר בתקנות חובת המכרזים, יהיה מנוע מלדרוש לעיין בחלק זה של ההצעה הזוכה בתיחור.
  3. יובהר כי:
     1. מענה המציע על מודל הייחוס ([נספח ד'](#נספח_ד)1), לרבות שמות הפריטים, מק"טים, תיאור הפריטים, מחירים וכמויות, לא יחשבו כסוד מסחרי או מקצועי.
     2. מענה המציע על הדרישות הטכניות ([נספח ג'](#נספח_ג)) ייחשב כסוד מסחרי או מקצועי ולא תתאפשר זכות עיון בחלק הזה של ההצעה הזוכה בתיחור.

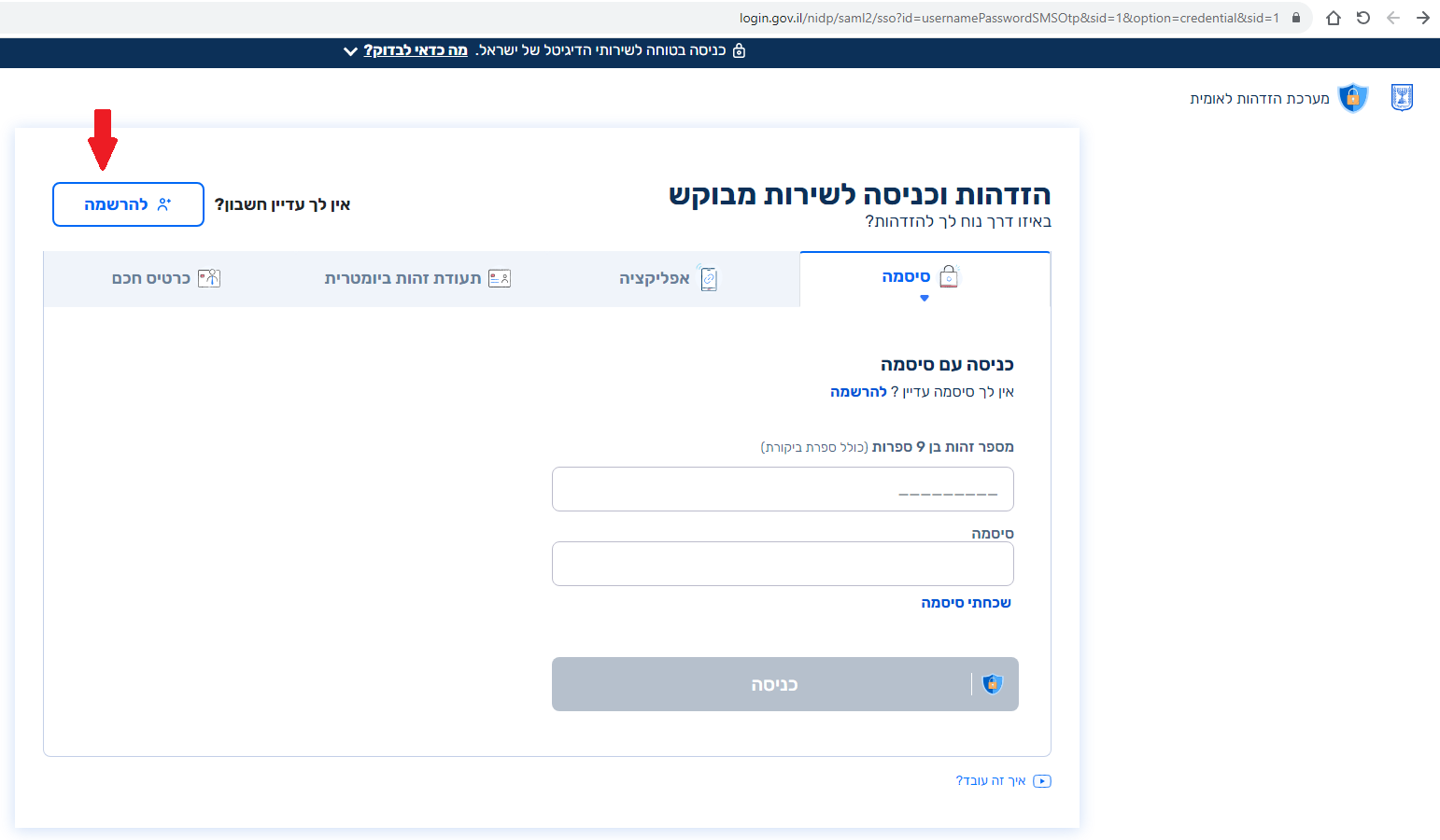
|  |  |  |
| --- | --- | --- |
| מס"ד | הסעיף/פרק במסמך התיחור | נימוק |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

\* **ניתן להוסיף שורות נוספות על פי המבנה המפורט לעיל.**

1. נספח ז' – הסבר על מערכת התיחורים הדינאמיים - מערכת מירב
   1. נספח זה בא להוסיף על האמור במסמכי המכרז המרכזי, ולא לגרוע מהם.
   2. נספח זה הינו עבור שלב התיחור הדינאמי המקוון ומהווה חלק בלתי נפרד ממסמכי המכרז המרכזי ומסמכי התיחור.
   3. בשלב זה – שלב התיחור הדינאמי המקוון – ישתתפו המציעים שנבחרו בהתאם לסעיף **שגיאה! מקור ההפניה לא נמצא.**‎1.4.3 ויתחרו בהתאם לכללים המפורטים בו.
   4. המסמכים הנדרשים לצורך התיחור הדינאמי פורטו בנספח 2 לחוברת 2 למסמכי המכרז המרכזי.
   5. **רישום למערכת ההזדהות הממשלתית (חד פעמי)** 
      1. הגשת הצעה תתאפשר, רק למי שיש לו משתמש במערכת ההזדהות הלאומית.
      2. רישום למערכת ההזדהות הלאומית, יבוצע בקישור הבא:

<https://account.gov.il/sspr/public/newuser>

* + 1. להלן סרטון הדרכה המסביר את אופן הרישום למערכת הזיהוי הממשלתית:   
       <https://www.youtube.com/channel/UCEflHGPEj-M7jtQ0PdzUZkQ>
    2. תהליך רישום והזדהות מול מערכות ממשלה שונות כמו גם מערכת מירב, מתבצע באמצעות 'מערכת ההזדהות הממשלתית'. רישום למערכת זו נעשה באמצעות מייל פרטי (כדוגמת Gmail) כפי שמופיע בתמונה. לתשומת ליבכם, הרישום ישמש אתכם גם לכניסה לשירותים ממשלתיים שונים לצרכיכם האישיים.



* + 1. בכל תקלה בהליך ההרשמה להזדהות הממשלתית, או בתהליך ההזדהות יש לפנות למוקד התמיכה של המערכת (טל - [1299](tel:1299), כתובת דואר אלקטרוני [moked@mail.gov.il](mailto:moked@mail.gov.il), טלפון נוסף [08-6863100](tel:08-6863100" \o "טלפון)).
  1. התיחור הדינאמי המקוון
     1. במסגרת התיחור, יתחרו המציעים על מתן מחיר המיטיב ביותר לעורך המכרז עבור הציוד, המוצרים והשירותים הנדרשים במסגרת המכרז.
     2. הצעת המחיר שתוגש על ידי המציע במסגרת התיחור תהיה סופית ותכלול את כל מרכיבי העלות של המוצרים והשירותים המבוקשים הנדרשים לצורך אספקתם וביצועם.
     3. הצעת המחיר במסגרת התיחור תחייב את המציע, ככל שיזכה במכרז, כמפורט במסמכי המכרז המרכזי ובמסמכי תיחור זה.
  2. מחיר מודל הייחוס
     1. עובר למועד התיחור, ולכל המאוחר עד 14 ימי עבודה לפני ביצוע התיחור הדינאמי המקוון, המציעים יגישו את מודל הייחוס ואת הסימולטור עם מחירי מחירון היצרן נכון למועד ההגשה, בהתאם לכתב הכמויות המפורט במודל הייחוס.
     2. ככל שימצא כי חל שינוי מהותי, על פי דעת עורך המכרז, בבסיס המחירון הרשמי של היצרן, לרבות שינוי מהותי בתצורות הציוד והשירותים, יהיה רשאי עורך המכרז לבקש לעדכן את מודל הייחוס בהתאם.
     3. המציע מחויב לעדכן את עורך המכרז מיד עם היוודע לו על שינוי מהותי בבסיס המחירון הרשמי של היצרן, או בסל המוצרים אשר התרחש לאחר הגשת הצעתו וטרם קיום התיחור. כמו כן, הוא מחויב ליידע את עורך המכרז בדבר מוצרים אשר, בהתאם להצהרת היצרן, קיימת היתכנות להפסקת ייצורם, שיווקם או התמיכה בהם (End Of Life, End Of Sale או End Of Support) או שכבר הוכרזו ככאלה, והכל כמפורט בחוברת המכרז הראשית.
     4. עורך המכרז יסכם עבור כל מציע מקבוצת המציעים הסופית אשר אושרו להשתתף בתיחור את מחיר ההצעה לפי מודל הייחוס, אשר יחושב בשקלים חדשים, לאחר המרתו מהמטבע הזר הנקוב במחירון היצרן, לפי השער היציג של המטבע הזר כפי שפורסם על ידי בנק ישראל 7 ימים לפני מועד התיחור הדינאמי המקוון, ויתווסף אליו מע"מ כדין, ככל שהמציע מחויב בגביית מע"מ (להלן: "**מחיר מודל הייחוס**"). מחיר מודל הייחוס יהווה את מחיר המקסימום להצעת הפתיחה של כל מציע בתיחור הדינאמי המקוון.
     5. מחיר מודל הייחוס יועבר למציע טרם התיחור לצורך בקרה כי לא נפלה טעות חשבונאית בהמרה שבוצעה על ידי עורך המכרז. יובהר כי מדובר בחישוב טכני ולא תינתן למציעים במכרז, בשלב זה של המכרז, כל אפשרות לשנות פרט מפרטי הצעתם.

1. נספח ח' – עיבוד ואבטחת מידע והגנה בסייבר בשירותים
   1. הגדרות
      1. **אירוע אבטחה** – אירוע (incident) אשר עלול לפגוע בזמינות, מהימנות או סודיות מידע מוגן או השירותים בהם משתמשים המזמינים לרבות תקיפת סייבר.
      2. **הוראה דיגיטלית** – הוראה שניתנה באמצעות כלי התאמה והגדרה (קונפיגורציה) כגון ממשק הניהול של הספק, APIs או כל אמצעי אחר שהועמד לרשות המזמין.
      3. **מידע מוגן** – נתוני עיבוד, נתוני גישה ונתוני תוכן.
      4. **נתוני גישה (Subscription Data)** – כל מידע של משתמשים ומזמינים הנדרשים לצורך ניהול גישה, אספקת השירותים או עבור ביצוע חיובים.
      5. **נתוני עיבוד** – כל מידע אשר נוצר במערכות הספק או היצרן במהלך או כתוצאה מעיבוד נתוני תוכן (מטא-דטא ולוגים), ואשר ניתן לייחוס בדרך כלשהי למזמין, לקבוצת מזמינים או למשתמש, ובכלל זה – זיהוי ופרטי המשתמש (לרבות שם, כתובת, פרטי חיוב, תאריך לידה, כתובת דוא"ל, מספר טלפון), תאריכי ושעות כניסה ויציאה מהמערכת (Log In ו-Log Out) מידע על המזמינים, שירותים המופעלים על ידם, נתוני וקובצי תצורה, הפעולות שבוצעו במערכות השונות, פרטי השימוש, כתובות IP שהוקצו על ידי ספקי שירותים (Access Data); Transactional Data ו-Traffic Data כולל מיקום גיאוגרפי (Geolocation) של מקור ויעד הנתונים, גודל הנתונים, מבנה הנתונים, מסלול, פרוטוקול תקשורת (Communication Protocol).
      6. **נתוני תוכן (Content data)** – הנתונים הדיגיטליים, ובכלל זה כל מידע, קובץ, מאגר, תוכנה, טלמטריה, לוגים, קוד, לוגיקה, נתון, דו"ח, סימן, טקסט, תמונה, אודיו, וידאו, צילום, וכיו"ב בכל פורמט, שהועלו, נוצרו במישרין על ידי משתמש או לבקשתו במערכות הספק או היצרן, לרבות בשירותי צד ג' בהם עושים הספק או היצרן שימוש.
      7. **עיבוד מידע** – פעולה או סדרת פעולות המתבצעות במידע בין אם באמצעים אוטומטיים ובין אם לא, כגון איסוף, הקלטה, ארגון, הבניה, אחסון, העברה, התאמה או שינוי, אחזור או שחזור, שימוש, הצפנה, הפצה או העמדה לעיון בדרך אחרת, יישור או שילוב, הגבלה, מחיקה או הרס וכיו"ב.
      8. **תקיפת סייבר –** אירוע אבטחה שמטרתו לעבור או לעקוף את אמצעי האבטחה או הבקרה בהם הספק, היצרן או המזמין עושים שימוש, או לנצל חולשה קיימת בניסיון לגרום לשיבוש של השירות או להרס, אובדן, דלף, שינוי, שימוש, חשיפה לא מורשית או גישה למידע מוגן.
      9. **Service Level Agreement (להלן: "SLA") –** הסכם בין ספק שירות למשתמש קצה אשר מגדיר את רמת השירות המצופה מספק השירות וקובע פיצויים בגין חריגה מרמה זו.
   2. חובה לאבטחת מידע והגנה בסייבר
      1. מבלי לגרוע מחובת הספק בכל מקום אחר, הספק יהיה אחראי על שמירה, הגנה ושלמות המידע המוגן על מערכותיו, והוא לא ייגש אליו, לא יאפשר לאחר לגשת אליו, לא יעשה בו שום שימוש או שינוי, ולא יתיר כל שימוש או שינוי, בין במעשה ובין במחדל, שאינו מותר בהתאם להוראות הדין הישראלי ובהתאם להוראת ההסכם ונספח זה.
      2. הספק יהיה אחראי לכך שלמזמינים ולמשתמשים תתאפשר גישה סדורה למידע המוגן, ובכל מקרה לא תימנע מהם גישה למידע כאמור, באופן הסותר את הוראת ההסכם או את הדין הישראלי.
      3. הספק מבין כי המידע המוגן כולל מידע אודות תהליכי העבודה של ממשלת ישראל וכן מידע שבחלקו נוגע באזרחי ותושבי מדינת ישראל. בהתאם, כל חשיפה, פגיעה, נזק, מניעת גישה, אובדן של מידע או חשיפה של מידע לצד שלישי עלול לגרום לעורך המכרז, למזמינים ולמשתמשים, וכן לצדדי ג' נזקים כבדים, ויהיה מחויב לשמור על המידע המוגן בהתאם לסטנדרטים הגבוהים ביותר הקיימים בשוק, ולא להעבירו לידי צד שלישי כלשהו, בהתאם להוראות נספח זה.
      4. מידע מוגן לא ישמר על תשתית ענן ציבורי שאינו אחד מספקי הענן הזוכים במכרז נימבוס.
      5. חובות הספק כלפי המידע המוגן יחולו כל עוד המידע מצוי במערכותיו או במערכות היצרן, גם לאחר תום תקופת ההתקשרות.
      6. הספק יאפשר שמירה ותיעוד מלא של כל גישה ושימוש של המזמין ומשתמשיו לשירותים השונים.
      7. תתאפשר שמירה של התיעוד לתקופה של שנה לפחות כך שיהיה זמין באופן רציף למזמין ולעורך המכרז.
   3. נתוני תוכן
      1. המזמינים יהיו רשאים לייצר נתוני תוכן במערכת או באמצעותה וכן להגר למערכת בענן כל נתוני תוכן שירצו, בכפוף להוראות הדין, ובכלל זה נתונים בעלי רמת רגישות שונה, כולל נתוני תוכן של מזמינים אשר חלות עליהם מגבלות שונות מכוח חוק, ולספק לא תהיה טענה או מגבלה על כך.
      2. בהתאם לדין הישראלי החל על נתוני תוכן של חלק מהמזמינים כפי שהוא מתעדכן מעת לעת, ישנן דרישות לגבי הגנה על המידע מפני שיבושו, שינויו או חשיפה לא מורשית שלו. בין השאר, הדינים החלים על מידע כוללים: חוק להסדרת הביטחון בגופים ציבוריים, התשנ"ח-1998, חוק עוולות מסחריות, חוק נכסי מדינה, וכן דינים ספציפיים החלים על פעילות המדינה ועובדי מדינה בתחומים שונים. החובות כלפי המידע המוגן בהתאם לכל דין מוטלות על המזמינים בלבד, שהם הבעלים של המידע, ולא כלפי הספק, אלא אם נקבע במפורש אחרת במסמכי המכרז. חובת הספק היא לעשות כל מאמץ סביר על מנת לאפשר למזמינים ולעורך המכרז לעמוד בחובות השונות החלות עליהם על פי כל דין ביחס למידע מוגן כאמור. אין באמור בסעיף זה כדי לגרוע מכל חובה החלה על הספק על פי דין.
   4. שימוש במידע
      1. עורך המכרז והמזמינים הם הבעלים הבלעדיים של המידע, והספק מהווה מעבד (Processor) של המידע והוא לא יעשה בו שום פעולה ובכלל זה שמירה ואחסון מידע, עיבודו והעברתו לכל גורם צד ג' אלא בהתאם להוראות הדין החלות במדינת ישראל ובהתאם למפורט להלן:
         1. בנתוני תוכן – באישור של המזמין, בהתאם להוראה דיגיטלית, ולצורך אספקה תקינה של השירותים הנרכשים.
         2. בנתוני עיבוד – ברמה המינימאלית הנדרשת לצורך אספקה תקינה של השירותים הנרכשים במסגרת ההסכם ובכלל זה שיפור הגנת הסייבר של מערכות הספק או השירותים, לחיוב בגינם ולמימוש חובותיו של הספק לפי ההסכם. יודגש כי שימוש בנתוני עיבוד לצורך שיפור השירותים של הספק שאינו חלק משיפור אותם השירותים עבור, בין היתר, המזמינים, אסור אלא במקרה של קבלת אישור בכתב של עורך המכרז.
         3. בנתוני גישה – ברמה המינימאלית הנדרשת לצורך אספקה תקינה של השירותים הנרכשים במסגרת ההסכם, לחיוב בגינם ולמימוש חובותיו של הספק לפי ההסכם.
      2. מבלי לגרוע מהאמור, ולמען הסר ספק, הספק לא ימכור, ישכיר או יבצע כל פעולה מסחרית אחרת במידע מוגן, ובכלל זה העברת המידע לאחר עיבוד, העברתו או מכירתו כחלק ממידע של משתמשים אחרים לאחר מחיקת פרטים מזהים, או בכל קונסטלציה אחרת, ללא אישור מראש ובכתב של עורך המכרז.
      3. לא ישמר מידע מוגן במערכות הספק או היצרן, שלא בהתאם להוראות ההסכם ונספח זה, ובהתאם להוראה דיגיטאלית, ויוודא ביעור של מידע כאמור שנמצא במערכותיו, בהתאם להוראות הדין.
      4. מבלי לגרוע מחובות הספק, הספק ינקוט באמצעי הזהירות הנדרשים על-מנת לוודא שהגישה למידע מוגן ניתנת אך ורק לגורמים מורשים מטעם הספק אשר גישה למידע זה נדרשת להם לצורך אספקת השירותים למזמינים. על הספק להבטיח כי החשיפה והשימוש במידע מוגן לגורמים המורשים יהיה במידה המינימלית המתחייבת לצורך אספקת השירות באופן תקין, ובהתאם לחובותיו של הספק. הספק ידריך את הגורמים המורשים במטרות השימוש במידע, ובאשר לחובות המוטלות עליהם בהתאם לדין ולהוראות הסכם זה כתוצאה מהחשיפה למידע.
   5. מחיקת מידע מוגן
      1. בתוך 30 יום מיום בקשת מזמין או תוך 90 יום מסיום ההתקשרות, מכל סיבה שהיא, יעביר הספק למזמין את כל המידע של המזמין, למעט אם המזמין הודיע שהוא אינו מעוניין במידע. ככל שהשירות מאפשר למזמין לאחזר מידע או למחקו ישירות, יאפשר הספק למזמין לבצע זאת עד 30 יום לאחר סיום ההתקשרות תוך מתן סיוע טכני סביר על ידי הספק לביצוע אחזור המידע או מחיקתו וכן להציג למזמין אסמכתאות כי אכן כלל המידע אוחזר או נמחק בהתאם לנדרש. כלל המידע יאוחזר בפורמט סטנדרטי, עדכני ולא קנייני.
      2. לאחר 90 יום ממועד סיום ההתקשרות, או בהתאם להוראה דיגיטלית למחיקת מידע ובהתאם לתנאי השירות, ימחקו, מחיקה מלאה, כל העותקים של נתוני התוכן במערכות או בסביבות השירותים בצורה שלא תאפשר שחזורם, אלא אם כן צוין אחרת בהסכם זה.
      3. בהמשך למפורט לעיל ובכפוף לחובותיו על פי כל דין, ימחקו כל נתוני עיבוד ונתוני גישה שאינם נחוצים לצורך ביצוע הפעולות המותרות המפורטות בסעיף זה מכל הרישומים והמאגרים.
   6. סודיות
      1. מוסכם על הצדדים כי המידע המוגן הוא סודי, ואין לעשות בו שימוש בניגוד להוראות ההסכם או להעביר אותו לידי אף גורם אחר ללא קבלת אישור מראש ובכתב של עורך המכרז.
      2. הספק מתחייב לשמור בסוד כלי אבטחה ובכלל זה כלי הצפנה כגון חותמות ומפתחות הצפנה אותם הוא מעמיד ברשות המזמין, ולא למסור לכל צד אחר כלים או סיוע טכנולוגי בפיענוח כלי האבטחה, ללא רשות מראש ובכתב של עורך המכרז.
      3. מבלי לגרוע מהאמור, הספק יהיה מחויב לנקוט בכל הצעדים הנדרשים ממנו לצורך שמירה בסודיות של נתוני גישה ונתוני עיבוד, אשר שמורים במערכות הספק באופן סודי ומאובטח, בכלל זה מתחייב הספק:
         1. כי נתונים אלו יוגנו באמצעים הטכנולוגיים המתקדמים ביותר הקיימים בשוק (State of the Art).
         2. כי הגישה לנתונים אלו על ידי עובדיו של הספק ייעשה רק על ידי מורשים הנדרשים לצורך כך ורק בהיקף המינימאלי הנדרש.
      4. הספק יישא באחריות כי מעבדי משנה מטעמו, אשר יקבלו ממנו גישה למידע מוגן לצורך מתן השירותים למזמינים, יהיו מחויבים לסודיות כמפורט בנספח זה, ובכל מקרה הוא יישא באחריות מלאה בגין כל הפרה שלהם של חובה זו.
   7. שירות ישראלי
      1. נתוני התוכן ישמרו במלואם בגבולות מדינת ישראל, אלא אם נקבע אחרת במסגרת הסכם זה.
      2. נתוני התוכן המצויים בתחומי מדינת ישראל לא יוצאו מחוץ לתחומי מדינת ישראל לשום צורך, ובכלל זה לעיבוד, לאחסון, לגיבוי או לצורך העברה לידי צד ג' ללא הוראה דיגיטלית מאת המזמין או באישור מראש ובכתב של עורך המכרז ובתנאים שיוגדרו על ידו.
      3. הוציא הספק מידע מוגן מחוץ לגבולות מדינת ישראל, ימחק את המידע המוגן באופן מידי, וככל שהדבר נעשה לצורך מתן שירות בהתאם להוראה דיגיטלית, מיד עם השלמת הפעולה, בהתאם לתנאי ההוראה הדיגיטלית, ובכפוף להוראות הדין.
      4. בכל מקרה ספק לא ישמור מידע מוגן במדינה שאינה מקיימת יחסים דיפלומטיים עם מדינת ישראל.
      5. האמור בסעיף זה יחול על שירות הפועל באזור חו"ל, בהתאמות הנדרשות.
   8. פרטיות
      1. מבלי לגרוע מחובותיו בנספח ובהסכם, הספק מתחייב לפעול בהתאם להוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "**חוק הגנת הפרטיות**") ותקנותיו וכל חקיקה אחרת בהתאם לדין הישראלי אשר מסדירה את עניין הפרטיות בהתאם לחוק הישראלי, על מנת לאפשר למזמינים להעלות מידע פרטי החוסה תחת החקיקה הרלוונטית (להלן: "**מידע פרטי**") לענן. יודגש בהקשר זה כי מזמינים שונים מחזיקים סוגים שונים ומגוונים של מידע מוגן ברמות שונות של רגישות לדוג', "מידע רפואי", כהגדרתו בחוק זכויות החולה, התשנ"ו-1996 מידע אישי, וכיוצ"ב.
      2. הספק יצרף לתנאי השימוש (service agreement) נספח ובו פירוט על העמידה בחובות המוטלות על הספק בהתאם לחוק הגנת הפרטיות ותקנותיו (להלן: "**נספח פרטיות**").
      3. הוראות נספח הפרטיות יקיימו, לכל הפחות את חובות הספק לפי הסכם ונספח זה. עורך המכרז יהיה רשאי לדרוש מהספק לבצע התאמות בנספח הפרטיות, לצורך התאמה להוראות החוק, ההסכם ונספח זה.
      4. הספק יעדכן את נספח הפרטיות, בהתאם לשינויים בדין החל בישראל ביחס למידע הפרטי שהמזמינים מחזיקים, באופן שיאפשר למזמינים להחזיק מידע פרטי בענן לאורך כל תקופת ההתקשרות.
      5. עבור שירות ישראלי, הספק לא יוציא מידע פרטי מגבולות מדינת ישראל, אלא במקרה של הוראה דיגיטלית של המזמין או באישור מראש ובכתב של עורך המכרז ובתנאים שיוגדרו על ידו.
      6. עבור שירות שאינו ישראלי, הספק לא יוציא מידע פרטי מגבולות אזור המצוי בגבולות האיחוד האירופי ויחולו עליו כללי ה- General Data Protection Regulation (GDPR).
      7. מבלי לגרוע מחובות הספק, הספק ישמור מידע מוגן הנתון תחת שליטתו הטכנית, כגון נתוני עיבוד או נתוני גישה בהתאם להוראות הדין ובפרט לפי חוק הגנת הפרטיות ותקנותיו.
   9. איסור פלילי על חשיפת מידע מוגן
      1. חשיפה או גילוי של מידע סודי לפי הסכם זה בין במעשה ובין במחדל שלא בהתאם להסמכה מפורשת ובכתב של עורך המכרז, מהווים הפרה של חובת הסודיות של הספק לפי הסכם זה, ומהווה עבירה פלילית לפי סעיף 118 לחוק העונשין, התשל"ז-1977.
      2. בנוסף, ובהתאם לסוג המידע שנחשף, גילוי של מידע מוגן, בין במעשה ובין במחדל, שלא בהתאם להוראות ההסכם או הוראות הדין, עלולה להוות עבירה פלילית בהתאם לחוק הישראלי, בהתאם לסוג המידע שייחשף (לדוגמא: מידע פרטי, מידע הנתון תחת חיסיון לפי החוק הישראלי, מידע שיש בו כדי לפגוע בביטחון המדינה וכיוצ"ב).
   10. דין חל וסמכות שיפוט על מידע מוגן
       1. **מבלי לגרוע מהאמור בסעיף 18 להסכם ההתקשרות**:
          1. למדינת ישראל יש אינטרס ריבוני מלא ובלעדי, וסמכויות וזכויות בעלות מלאות במידע המוגן. ככזה, הדין שיחול על מידע מוגן הוא הדין של מדינת ישראל, וקיימת סמכות בלעדית לבתי המשפט של מדינת ישראל לדון בכל שאלה או הליך הנוגעים למידע האמור, ללא סייגים או החרגות.
          2. בכל סכסוך ישיר בין הספק לעורך המכרז הנוגע למידע מוגן יהיה הדין החל הדין הישראלי וסמכות השיפוט תהיה באופן בלעדי לבתי המשפט של מדינת ישראל לדון בכל שאלה או הליך הנוגעים למידע האמור, ללא סייגים או החרגות.
       2. הספק יודיע באופן מידי על שינויים או עדכונים במצב המשפטי החל עליו, המשפיע על מימוש החובות והזכויות ביחס למידע מוגן לפי הסכם זה. למען הסר ספק, לא יהיה בשינוי כאמור כדי לפטור את הספק מחובותיו בהתאם להוראות ההסכם.
   11. העברת מידע שלא כדין
       1. על אף האמור בסעיף ‎9.10.1 לעיל, היה והתקבל צו של ישות זרה לצורך קבלת מידע מוגן, מחיקתו, שינויו או מניעת גישה אליו, ולדעת הספק הפניה או הצו כאמור מחייבים אותו משפטית, בין אם המידע מצוי בתחומי מדינת ישראל ובין אם לאו, יפעל הספק בהתאם למפורט להלן:
          1. יודיע על הפניה או הצו בהקדם האפשרי לעורך המכרז והמזמין הרלוונטי, ויעדכן אותם על הצעדים שננקטו על ידו עד שלב זה, וזאת למעט אם נאסר עליו מפורשות על פי דין לעשות זאת.
          2. ככל שישנו צו חיסיון על עצם הבקשה לקבלת המידע, יפעל הספק להסרת הצו, ולמתן אפשרות ליידוע של עורך המכרז על עצם קיומה של הבקשה.
          3. יסרב להעברת המידע, ויטען את כל הטענות המשפטיות הרלוונטיות ובכלל זה שהמידע שייך למדינה ריבונית, וכן שהמידע נתון תחת חסינות מדינתית.
          4. במידת הצורך יגיש ערעור על ההחלטה לערכאה השיפוטית או לרשות המנהלית הרלוונטית ועד למיצוי כלל ערכאות הערעור האפשריות, תוך הגשת בקשה לעיכוב הביצוע עד הכרעה סופית בנושא.
          5. בהתאם לבקשה של עורך המכרז, יבקש לצרף את ממשלת ישראל כצד להליך הרלוונטי.
          6. ידאג לצמצם את היקף חשיפת המידע אך ורק למידע רלוונטי בבקשה.
          7. ידרוש כי מילוי אחר הפניה או הצו יהיה בהתאם לאמנות בינלאומיות לסיוע משפטי (Mutual Legal Assistance Treaties), ולא ימלא אחר הפניה או הצו אלא אם כן הדבר מתאפשר לפי דין המקום בו המידע המוגן מצוי.
       2. בנוסף לאמור לעיל, ככל שתתקבל פניה או צו של ישות זרה לצורך קבלת מידע מוגן המצוי במדינת ישראל, ולדעת הספק הצו כאמור מחייב אותו משפטית, בנוסף למפורט בסעיף ‎9.11.1 לעיל, יפעל הספק כמפורט להלן:
          1. הספק יפעל בהתאם להוראות הדין הישראלי לצורך אכיפת הצו (כגון לפי חוק אכיפת פסקי-חוץ, תשי"ח-1958, חוק עזרה משפטית בין מדינות, תשנ"ח-1998, וכיוצ"ב).
          2. בכל מקרה הספק לא יאכוף צו שניתן על ידי ארגון של מדינה זרה על מידע מוגן של ממשלת ישראל, הנתון בשטחי מדינת ישראל, ללא שהדבר מתאפשר לפי הדין הישראלי.
       3. מבלי לגרוע מחובות הספק בכל מקום אחר, האמור בסעיף זה יחול על הספק גם במידה והפניה מיישות זרה התקבלה אצל מעבד משנה או קבלן משנה אחר המופעל על ידו לצורך אספקת השירותים מכוח ההסכם, והמחזיק בידו את המידע המוגן. במקרים כאמור יכנס הספק בנעלי המעבד או קבלן המשנה שלו ויפעל בהתאם לחובות אלו.
       4. ככל שיש לספק אינדיקציה על כך שצפויה להתקבל פניה או צו כאמור בסעיפים ‎9.10.1-‎9.11.1 לעיל, הוא יתריע על כך בפני עורך המכרז באופן מידי, אלא אם הוא מנוע על פי דין.
   12. פעולות נדרשות במקרים של העברת מידע מוגן
       1. מבלי לגרוע מאחריות הספק לפי כל דין, ומבלי לצמצם את חובתו לפי הסכם זה, בכל מקרה בו העביר הספק מידע מוגן לידי צד שלישי שאינו מורשה לקבלו בהתאם לכללי המכרז, מכל סיבה שהיא, ובכלל זה כתוצאה מפניה או צו של ישות זרה יפעל הספק בהתאם למפורט להלן:
          1. הספק יידע את עורך המכרז בהקדם האפשרי ובאופן מיידי על כל מידע מוגן שנמסר על ידו כאמור, על היקף המידע, על זהות מקבל המידע, על הסיבות למסירת המידע, האם המידע היה מוצפן או מוגן בכלי אבטחה נוספים וכל מידע רלוונטי נוסף, וזאת למעט אם נאסר עליו על פי דין לעשות זאת.
          2. הספק לא ינקוט בפעולה כלשהי שיש בה כדי לסייע לפענח או להסיר כל חסם טכנולוגי ממידע מוגן בשום צורה ובשום אופן בין במעשה ובין במחדל. התקבלה בקשה כאמור מרשות אכיפת חוק או רשות ביטחון של מדינה זרה לפיענוח או הנגשת מידע מוגן, יפנה הספק לעורך המכרז לצורך קבלת אישור למתן סיוע כאמור, ויפעל בהתאם להנחיות עורך המכרז.
          3. הועבר המידע המוגן וזאת מבלי לידע את עורך המכרז (בין אם יצא צו המונע את עצם גילוי הדרישה להעברת המידע, בין אם מדובר בדרישה של רשות ביטחונית ובין אם מכל סיבה אחרת) ישלם הספק לעורך המכרז פיצוי מיוחד בסך של 7,555 ₪ וזאת תוך פרק זמן של עד 24 שעות מרגע מסירת המידע.
       2. אין באמור בסעיף זה כדי לגרוע מאחריות הספק, והחובה שלו על פי דין ועל פי הוראות ההסכם לא למסור מידע מוגן ללא הסכמה מראש ובכתב של עורך המכרז וכן אין בה כדי לגרוע מכל זכות לפיצוי, שיפוי או לכל תרופה אחרת הנתונה בידי עורך המכרז, בהתאם למפורט בהסכם.
   13. חובת הספק לאבטחת מידע וסייבר
       1. הספק יהיה האחראי הבלעדי על אבטחת המערכות עליהם מבוססים השירותים המוצעים על ידו למזמינים, בין אם ישירות, בין אם על ידי מעבד משנה ובין אם באמצעות הסכם תואם עם ספק הענן עליו השירות פועל, ידאג לתפעל ולעדכן את אמצעי האבטחה באופן שוטף, ויוודא כי האמצעים הטכנולוגיים המשמשים לאבטחת המידע הם חדישים (state of the art) ועומדים בסטנדרט הגבוה ביותר המקובל בשוק.
       2. הספק יהיה אחראי להגן על מערכותיו, לרבות תשתית ייעודית, וכן על השירותים המוצעים על ידו אל מול איומים ותקיפות סייבר וכל ניסיון לפגוע או לחסום גישה לתשתיות אלו. במסגרת כך, הספק יינטר את מערכותיו ויפעל לאתר חולשות במערכותיו ולטפל בהן ולעדכן את מערכותיו מפני חשיפות אבטחתיות בהקדם האפשרי תוך הפעלת תהליכי מיטיגציה (Mitigation) ככל ולא ניתן לעדכן את המערכות באופן מידי.
       3. הספק יקצה נציג אשר יהיה אחראי לפניות בנוגע לאבטחת מידע והגנה בסייבר, ביצוע ביקורות, אספקת אסמכתאות כנדרש בהסכם, התראות על איומים והתמודדות עם אירועים בזמן אמת. ככל שספק השירות מפעיל חדר מצב להתמודדות עם איומים בסייבר (SOC), הנציג יעביר את פרטי הקשר עם חדר מצב זה לעורך המכרז.
       4. אחריות הספק לאבטחת מידע והגנת סייבר, תבוא לידי ביטוי, בין היתר בעמידה בעקרונות הבאים ככל שהם רלוונטיים למתן השירותים:

|  |  |
| --- | --- |
| 1. **ניהול כוח אדם והדרכה** – וידוא כי מועסקים ועובדי קבלן מכירים ומבינים את אחריותם בתחום מדיניות אבטחת מידע והגנת הסייבר. | 1. **ניהול שרשרת אספקה וספקים –** הגדרה וקיום מנגנונים שתפקידם לנהל את כל שרשרת האספקה של ספק הענן כדי להבטיח את אמינות התשתיות שבאמצעותן מסופקים השירותים. |
| 1. **ניהול משאבים –** קיום מנגנונים לזיהוי והגנה על נכסים ארגוניים ונכסי מידע ארגוניים, כולל אלה של לקוחות והמזמין. | 1. **ניהול אירועי וחשדות לאירועי אבטחה –** קיום אמצעים לניהול, תגובה והעברה של מידע על אירועי אבטחה. |
| 1. **ניהול זהויות והרשאות גישה –** קיום מנגנונים לווידוא כי הגישה למידע מוגן, משאבי עיבוד מידע, מתקנים וסביבות וירטואליות הן של משתמשים מורשים בלבד. | 1. **רציפות תפקודית והתאוששות –** להבטיח את הרציפות התפקודית של שירותי הענן, כולל התאוששות מאסון תוך הבטחת מהימנות ואמינות המידע בכל עת. |
| 1. **הצפנה וניהול מפתחות –** קיום פעילות מאובטחת של שירותי הספק באמצעות הגדרה ומימוש של מנגנונים קריפטוגרפים נאותים. | 1. **קיום מנגנוני הערכת רמת אבטחה –** להקים ולנהל תהליכים מתאימים לבדיקת רכיבי מפתח ברשת ובמערכות המידע התומכות את שירותי הענן ולהקים ולנהל תהליכים מתאימים כדי להעריך את רמת ההגנה על נכסים קריטיים**.** |
| 1. **אבטחה פיזית וסביבתית –** קיום אמצעים למניעת גישה לא מורשית לאתרים הפיזיים כדי למנוע נזק, אובדן, פגיעה, תקלה, או גניבה של הנכסים הארגוניים שעלולים לפגוע בפעילות הספק. | 1. **שמירה על יכולת הגירה ואינטראופרביליות –** להקצות ללקוח אמצעים שמאפשרים להתממשק לשירותי ענן אחרים או להגר, באופן מאובטח לספקים המספקים שירותים דומים. |
| 1. **שמירה על רציפות תפקודית תפעולית מאובטחת –** וידוא כי מערך הגנת הסייבר של הספק פועל מאובטח ותקין כדי ששירותי הענן יהיו מבצעיים כל העת. | 1. **הגנה על שלמות ואמינות המערכת –** להקים ולנהל את האמצעים המתאימים להבטיח שהמערכת שומרת על רמת הגנה ומהימנות נאותה בכל מחזור החיים מפיתוח לפריסה מבצעית, כולל פיתוח פנימי ופיתוח חיצוני, תוך שימוש בכלים מסחריים ובכלי קוד פתוח. |
| 1. **אבטחת תקשורת –** אבטחה של התקשורת הממוחשבת. | 1. **ניהול סיכונים –** להקצות את האמצעים הנדרשים לממשל וניהול סיכוני מידע, וכן מנגנונים לאיתור סיכונים להגנת שירותי הענן. |
| 1. **הגנה על מידע אישי –** להקים ולנהל את האמצעים הנדרשים כדי שהמזמינים יממשו את חובותיהם להגן על המידע המצוי בשליטתם. | 1. **הליכים נאותים להערכת הגנת הסייבר –** להקים ולנהל תהליכים נאותים לבדיקות הליכי בקרת אבטחה של מערכות ורשתות ליבה של תשתית הענן. |
| 1. **ניהול קונפיגורציה ושינויים –** להקים ולנהל מערכות לניהול שינויים לרשת ולמערכות מידע. | 1. **פיתוח מאובטח** – להקים ולנהל את האמצעים המתאימים על מנת להבטיח כי כלל מחזור החיים של פיתוח המערכות מבוצע במתודות של פיתוח מאובטח, כגון מתודת SDLC. |

* 1. נהלי הגנת סייבר וניהול סיכונים
     1. הספק יקבע נהלי אבטחה בתחום הסייבר, בהתאם לחובת הספק לאבטחת המידע והגנת סייבר המפורט לעיל, ולצורך התמודדות עם תרחישי ייחוס ואיומים על תשתיות הענן ועל השירותים המסופקים על בסיס תשתיות אלו (להלן: "**מדיניות הסייבר של הספק**").
     2. הספק יבצע הליכי ניהול סיכונים בהתאם לדרישות התקנים בהם הוא עומד ולדרישות החוקים והרגולציות החלות עליו, באופן שוטף.
  2. תקנים
     1. תקנים בינלאומיים מקובלים מהווים מסגרת בסיסית מינימלית לתשתית הגנת סייבר הנדרשת אצל הספק. על הספק יהיה לעמוד בתקינה בינ"ל מקובלת בתחום אספקת השירותים הניתנים על ידו.
     2. מבלי לגרוע מהאמור, שירות ישראלי יעמוד לפחות בתקנים אותם יש לספק באזור חו"ל. ככל שלא ניתן לקבל את תו התקן הרלוונטי בישראל, על הספק לעמוד בדרישות התקן במלואן אף ללא קבלת האסמכתא הרשמית.
     3. בהתאם לדרישת עורך המכרז, יציג הספק את האסמכתאות הרשמיות לעמידתו בתקנים הנדרשים. במקרה בו אין אפשרות לאסמכתה רשמית יציג הספק את תהליך הבקרה שנעשה לצורך עמידה בתקינה הרלוונטית, ובהתאם לדרישת עורך המכרז, יציג אישורים מטעם גורם חיצוני בלתי תלוי בעל הכשרה רלוונטית, ובמתודולוגיה מקובלת.
     4. ככל שתקנים אלו יתעדכנו או שתצא להם גרסה חדשה, יהיה הספק מחויב לעדכנם בהתאם.
     5. הספק יעדכן באופן פומבי את התקנים להם השירות הוסמך.
  3. עדכונים שוטפים והעברת מידע בנושאי איומי סייבר
     1. הספק ישתף פעולה עם עורך המכרז בנושא ההגנה מפני איומי סייבר, וזאת כחלק ממתן השירותים, בהתאם למפורט להלן:
        1. עורך המכרז יעביר, בכפוף למגבלות החלות עליו ולמדיניות מסירת מידע שיגבש, מידע שיש בו כדי לסייע לאבטחת המידע והגנת הסייבר בהתאם להוראות ההסכם, ובכלל זה מידע אודות איומי סייבר, שיטות, תבניות לתקיפה וטכנולוגיות אשר ייתכן ויופנו כלפי המזמינים או הספק בקשר עם אספקת השירותים למזמינים.
        2. הספק יעביר בהקדם האפשרי, בכפוף למגבלות החלות עליו ועל פי כל דין, מידע שיש בו כדי לסייע למזמינים ולעורך המכרז לאבטחת המידע והגנת הסייבר ובכלל זה מידע אודות איומי סייבר, שיטות, תבניות לתקיפה וטכנולוגיות אשר מהווים סיכון למידע מוגן ולשירותים הנרכשים על ידי המזמינים.
  4. התמודדות עם אירועים בזמן אמת ותחקור אירוע
     1. הספק יאפשר לעורך המכרז ולמזמינים שימוש בשירותי חקר ו-IR (Incident Response) של הספק, ככל ושירותים אלו מוצעים על ידי הספק, לצורך התמודדות עם אירועי אבטחה ותקלות או חקירה ותחקור של אירועים אלו. ככל ואין לספק צוות IR ייעודי, יסייע הספק למזמין בהתמודדות עם האירוע על ידי הצוות ההנדסי של החברה או גורמים חיצוניים המופעלים על ידו.
     2. הספק יידע את המזמינים, ככל הניתן, בזמן אמת על אירועי אבטחה, ובכלל זה על תקיפת סייבר ועל ניסיונות לתקיפת סייבר על מערכות המזמין ועל תשתיות הספק אשר עליהן מופעלות מערכות ונתוני המזמינים.
  5. מהימנות עובדים וספקים
     1. הספק יבצע תהליכים מקובלים לבחינת רמת המהימנות של עובדיו, קבלני משנה וספקיו תוך הפעלת תכנית לאיתור ומענה לאיומי אבטחה אשר מקורם בגורם הפנימי.
     2. **מעבדי משנה**
        1. הספק יהיה רשאי למלא את החובות המוטלות עליו מכוח ההסכם באמצעות מעבדי משנה. כל החובות המוטלים על הספק מכוח ההסכם ובכלל זה נספח זה יחולו במלואם על מעבדי המשנה המאושרים. בכל מקרה של הפרה של חובות הספק באמצעות מעבד משנה, הספק יישא באחריות מלאה על הפרה זו.
     3. **הנחיות להפעלת מעבד משנה**
        1. הספק יגביל את יכולת הגישה של מעבד המשנה למידע של הלקוח למינימום הנדרש לצורך מתן השירות או המשך מתן השירות למזמינים או למשתמשי הקצה. הספק ימנע ממעבד המשנה גישה למידע לכל מטרה אחרת.
        2. מעבד המשנה וכל הגורמים המורשים מטעמו לגשת למידע מוגן יהיו חתומים על התחייבות לשמירה על סודיות שתעמוד בחובות הסודיות החלות על הספק.
        3. מעבד המשנה עמד בחובה המפורטת בסעיף ‏‎9.4.4 לעיל, הקובע כי גישה למידע מוגן יעשה רק לעובדים שהדבר הכרחי עבורם, ורק בהיקף חשיפה בהתאם.
        4. הוצאת המידע למעבד משנה אינה אסורה בהתאם לדין (כגון הדין החל לעניין פרטיות וכיוצ"ב).
        5. הספק יבצע ביקורות עיתיות לספקי המשנה המספקים שירותים למזמינים.
  6. אבטחת מידע בשירותים
     1. הספק יוודא כי רמת ההגנה והמהימנות של השירותים המסופקים על ידו תהיה גבוהה ותתעדכן ותשודרג לכל אורך תקופת ההתקשרות. הספק לא יבצע שנמוך (Downgrade) לרמת ההגנה של השירותים, ללא הודעה מראש לעורך המכרז.
     2. כל השירותים המאושרים יעמדו בתקני אבטחת מידע וסייבר הרלוונטיים, והמקובלים בשוק. עורך המכרז יהיה רשאי לבקש אסמכתאות לעמידת שירות מסוים בתקנים כאמור, ובשירותים שעדיין אינם עומדים במבחני תקן רשמי יעביר הספק את פירוט הבדיקות הפנימיות ומעבדות צד ג' שבחנו את רמת השירות, ובכלל זה את מתודולוגיות הבדיקה וההסמכות של מבצעי הבדיקות. עורך המכרז יעדכן את מדיניות הסייבר שלו לגבי השירותים המאושרים, בין היתר, בהתבסס על ההוכחות שיועברו על ידי הספק.
     3. לספק לא תהיה כל גישה לשינוי, החלפה או צפייה במידע אודות מפתחות ההצפנה של המזמין, ככל שישנם, ולא יעשה בהם שימוש כלשהו מבלי לקבל את אישורו מראש ובכתב של עורך המכרז.
     4. הספק לא ימנע כל שימוש של המזמין בכלי הגנת סייבר ואמצעים הנדרשים לאבטח את השירותים, ובכלל זה מנגנוני הצפנה המופעלים על ידו, ככל שאין בכך בכדי לפגוע באספקתו התקינה של השירות.
        1. **ביקורות תקופתיות** 
           1. אחת לתקופה, בהתאם לניהול הסיכונים של הספק, או כמענה לבקשת עורך המכרז ובתיאום עם הספק, יערוך הספק ביקורת חיצונית של חברה עצמאית ומובילה המתמחה בבחינה כאמור (להלן: "**חברת ביקורת**") לצורך וידוא עמידת הספק בהוראות המכרז או לחילופין, יאפשר לעורך המכרז לבצע ביקורת כאמור. דרישה של עורך המכרז לביקורת חיצונית תיעשה לכל היותר פעם בשנה, למעט אם מדובר בהתמודדות עם אירוע אבטחה. הספק ידון בדוחות הביקורת שיועברו אליו בתום הביקורת ויבחן את הצורך בעדכון נוהל האבטחה בעקבותיהם.
           2. לבקשת עורך המכרז, ובהודעה מראש לספק, תערוך חברת ביקורת שתאושר על ידי עורך המכרז, ביקורת מיוחדת, נוכח אירוע אבטחה או שינויים בנהלי ושיטות האבטחה של הספק.
           3. עורך המכרז יוכל לדרוש לקבל מידע אודות חברת הביקורת, ההסמכות שיש לה, וכן פרטים אודות מבצעי הביקורת בשמה. עורך המכרז יוכל לדרוש מהספק להחליף את חברת הביקורת, וזאת במקרים בהם נמצא כי יש חשש מבוסס לכך שהחברה אינה מבצעת את תפקידה כנדרש.
           4. לבקשת עורך המכרז, הספק יעביר לעורך המכרז את תמצית ממצאי הביקורת ואת סטטוס הטיפול בממצאים.
           5. הספק יישא בעלות הביקורות כאמור.
        2. **מבדקי בטחון וחדירות** 
           1. עורך המכרז יהיה רשאי לבצע בקרה על מימוש המדיניות המוגדרת על ידו למזמינים ועל אופן מימושה על תשתיות הספק.
           2. בדיקה זו תתבצע הן ברמת בדיקת ההגדרות ותצורת המערכות כפי שהוגדרה על ידי המזמין והן על ידי ביצוע מבדקי עמידות למערכות **המזמין** המופעלות על מערכות ותשתיות הספק.
           3. על מנת למזער את הסיכונים הכרוכים במבדקים אלו, מבדקי העמידות יתואמו מראש עם הספק תוך שהספק יימנע מלחסום את הגורמים הבודקים.
  7. תקיפת סייבר ואירוע אבטחה
     1. בכל מקרה בו אותרה תקיפת סייבר או כל אירוע אבטחה במערכות הספק היכולות להשפיע על המזמינים, ינקוט הספק בפעולות הבאות:
        1. הספק יידע בהקדם האפשרי את המזמין ועורך המכרז ובהתאם לחומרת האירוע, ובכל מקרה בפרק זמן שלא יעלה על 12 שעות מהרגע בו איתר באופן וודאי את אירוע תקיפת הסייבר, זאת למעט במקרה בו ניתן צו של ערכאה שיפוטית מוסמכת האוסר זאת.
        2. הספק ינקוט בכל צעד הנדרש, בהתאם לנסיבות העניין, כדי להפחית את ההשפעות ולמזער את הנזק הנובע כתוצאה מתקיפת הסייבר.
        3. הספק יידע את המזמין ועורך המכרז על צעדים שהם יכולים לבצע כדי להפחית את ההשפעות ולמזער את הנזק הנובע כתוצאה מאירוע האבטחה.
        4. הספק יבצע תחקור של אירוע התקיפה ויעביר את ממצאי התחקיר לעיון המזמין ועורך המכרז. התחקיר יכלול מידע בהתאם לכללים מקובלים של שיתוף מידע בתחום הסייבר.
     2. הספק ידווח, באופן שוטף, למזמין ולעורך המכרז, על פעולות שהוא ניטר אותן כניסיונות לתקיפת סייבר הממוקדת במערכות המזמינים.
     3. הספק יפיק לקחים מאירועי האבטחה שאירעו ויבחן את הצורך בעדכון המערכות, התהליכים והנהלים.
     4. במקרה בו אירע אירוע אבטחה במערכת מסוג תוכנה כשירות, הספק ישפה את המזמין או עורך המכרז, בכפוף להוראות סעיף 9.3 להסכם ההתקשרות, עבור כל הוצאה סבירה ומתועדת אשר נועדה לחקור, להחיל, לצמצם, לתחום ולתקן את הפגיעה בסודיות, תקינות וזמינות המידע של המזמין לרבות תהליכי הודעה והסגרה של האירוע לרשויות הרלוונטיות.