מדינת ישראל - משרד האוצר

אגף החשב הכללי - מינהל הרכש הממשלתי

מכרז מרכזי 2022-05

תיחור מס' 6 לאספקת מוצרי SSE (Secure Service Edge) ושירותים נלווים עבורם

גרסה 3 ~~2~~ – מרץ 2024

1. כללי התיחור

1.1. כללי

1.1.1. מינהל הרכש הממשלתי באגף החשב הכללי, משרד האוצר (״**עורך המכרז**״), מפרסם תיחור לאספקת מוצרי SSE – Secure Service Edge ושירותים נלווים עבורם (״**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 (״**המכרז המרכזי**״) והוא יסומן כתיחור מס׳ 6.

1.1.2. רשאים להשתתף בתיחור רק ספקי המסגרת. במסמך זה, יכונו ספקי המסגרת גם כ״מציע״.

1.1.3. **אין להפיץ את מסמכי התיחור לאף גורם מלבד הגורמים הנדרשים לצורך המענה לבקשה זו** ובכפוף להתחייבותו של אותו גורם, לשמירה על סודיות מסמכי התיחור.

1.1.4. את המענה לתיחור זה יש להגיע עד למועד המפורט בנספח א׳ – פרטים כלליים לתיחור.

1.1.5. 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.

1.1.6. התיחור יערך בשיטה של תיחור דינאמי מקוון. אם תשתנה שיטת התיחור, יודיע על כך עורך המכרז מראש לספקים הרשומים תוך זמן סביר אשר יאפשר הגשת הצעות כספיות לתיחור.

1.1.7. בתיחור זה ייבחר **זוכה יחיד** (״**הזוכה**״) אשר יהיה רשאי לספק את כל קו המוצרים והשירותים הכלולים בתיחור זה.

1.1.8. 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 באישור ועדת הפטור כהגדרתה בתקנות חובת המכרזים, תשנ״ג – 1993.

1.1.9. 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. במקרה כאמור, ישלח עורך המכרז מסמכי תיחור מעודכנים. פרסם עורך המכרז מהדורה מעודכנת של מסמכי התיחור, על המציע להקפיד על הגשת המענה על פי הנוסח המעודכן.

1.1.10. **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.

1.1.11. אשת הקשר לתיחור זה היא דניאל בן-חמו, בכתובת דוא״ל: GPA_cyber@mof.gov.il.

1.1.12. בכל פנייה בנושא תיחור זה, יש לציין בכותרת המייל את מס׳ התיחור, שם התיחור ונושא הפנייה (לדוגמא: ״**תיחור מס׳ 6 – שירות SSE – שאלות הבהרה**״).

1.1.13. 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.

1.2. שאלות הבהרה והערות

1.2.1. הגשת שאלות הבהרה והערות

1.2.1.1. שאלות הבהרה והערות לתיחור זה יש לשלוח לכתובת הדוא"ל המפורטת בסעיף 1.1.11~~1.1.11~~ לעיל, וזאת עד למועד האחרון להגשת שאלות הבהרה והערות, כמפורט בנספח א' – פרטים כלליים לתיחור.

1.2.1.2. השאלות תוגשנה אך ורק על גבי קובץ ה-Excel המצורף להודעת עורך המכרז על פרסום התיחור ("**הודעת פרסום התיחור**") ומסומן כנספח א'1.

1.2.1.3. 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.

1.2.1.4. שאלות שיועברו לאחר המועד או שיופנו בעל פה, בטלפון או בפורמט אחר מהנדרש לא יחייבו מענה על ידי עורך המכרז.

1.2.1.5. לא ייתן מענה לשאלות שישלחו בעילום שם.

1.2.1.6. עורך המכרז רשאי לאפשר סבבים נוספים של שאלות הבהרה והערות, בהודעה שתפורסם לספקי המסגרת.

1.2.1.7. 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.

1.2.2. מענה עורך המכרז לשאלות הבהרה והערות

1.2.2.1. תשובות והבהרות תינתנה בכתב בלבד. נוסחן הוא הנוסח המחייב והן יהיו חלק בלתי נפרד ממסמכי התיחור.

1.2.2.2. 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.

1.2.2.3. עורך המכרז רשאי לבצע כל שינוי במסמכי התיחור, וכן ליתן פרשנות או הבהרה להוראות המכרז והתיחור, גם ללא קשר לשאלות הבהרה.

1.2.2.4. עורך המכרז אינו מחויב לנוסח שאלה שהוגשה, ובכלל זה רשאי עורך המכרז, בעת ניסוח מענה לשאלות ההבהרה, לקצר נוסח של שאלה או לנסחה מחדש.

1.2.2.5. זהות השואלים לא תפורסם במסגרת המענה לשאלות ההבהרה או בכלל, למעט על פי חובה שבדין.

1.3. הגשת הצעות

1.3.1. כללי

1.3.1.1. המציע יגיש הצעה **אחת** למוצריו ושירותיו **של יצרן אחד**.

1.3.1.2. 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.

1.3.1.3. 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').

1.3.1.4. ההגשה תתבצע לתיבת מכרזים דיגיטלית, כאמור בסעיף 1.3.2 להלן.

1.3.1.5. המסמכים שיוגשו במסגרת המענה לתיבת המכרזים הדיגיטלית:

שם המסמך	**הערות**
אישור המציע	חתום ע"י מורשה חתימה מטעם המציע, בנוסח המצ"ב כנספח ב'. *** יוגש בפורמט PDF**
דרישות מקצועיות וטכניות	מענה מלא לשאלות המפורטות בנספח ג'. *** יוגש בפורמט WORD** *** כל מסמך שברצון המציע להגיש, יש לצרף למענה ולהפנות לחלקים המתאימים במסמך.** *** קישורים לא ייבדקו.**
מחירון	המחירון הרשמי של היצרן. *** יוגש בפורמט PDF** *** על המחירון הרשמי להיות מחירון מחוז קולומביה, חתום כנדרש, הכל לפי האמור בסעיף 3.7.1 למסמכי המכרז המרכזי.**
מפרט רישוי	מפרט רישוי מלא של היצרן עבור כל המוצרים הכלולים במחירון הרשמי שלו. *** יוגש בפורמט PDF**
מודל ייחוס	בהתאם למפורט בנספח ד'1 המצורף להודעת פרסום התיחור. *** יוגש בפורמט EXCEL** *** יש לשים לב להוראות סעיפים 3.7.4 ו-3.7.5 למסמכי המכרז המרכזי.**
הצהרת יצרן	בהתאם לנוסח המצ"ב כנספח ה'. *** יוגש בפורמט PDF** *** ניתן להגיש את ההצהרה בשפה העברית או האנגלית.**
בקשה לחיסיון פרטים מתוך ההצעה	בהתאם לנוסח המצ"ב כנספח ו'. *** יוגש בפורמט Word.**
מינוי נציג למערכת מיר"ב	בהתאם לנוסח המצורף כנספח 1 לחוברת מס' 2 למסמכי המכרז. *** יוגש בפורמט PDF.** *** יוגש רק במקרה שהמציע מבקש לשנות את הנציג מטעמו**
מסמכים נוספים	אם הדבר נדרש, ניתן לצרף נספחים למענה, לרבות אישורים, פרוספקטים וכדו'.

* יוגשו בפורמט בו נערכו מקור.	

1.3.2. **הגשת הצעות בתיחור**

1.3.2.1. הגשת ההצעות לתיחור תבוצע באופן מקוון, באמצעות **מערכת יהלום**, אלא אם כן קבע עורך המכרז בהודעה שתפורסם לספקי המסגרת דרך הגשה אחרת. במקרה כאמור על המציעים לפעול בהתאם להוראות שפורסמו.

1.3.2.2. קישור למערכת לצורך הגשת הצעות ישלח באמצעות דוא"ל וישלח לרשימת ספקי המסגרת. מציע אשר מעוניין לשאול שאלות הבהרה ולהגיש את הצעתו לתיחור, נדרש ללחוץ על הקישור "להגשת שאלות והצעות" במערכת יהלום.

1.3.2.3. הליך הגשת ההצעות במערכת כולל 2 שלבים:

1.3.2.3.1. הזדהות של מגיש ההצעה באמצעות מערכת ההזדהות הלאומית.

1.3.2.3.2. הגשת ההצעה בתיבת המכרזים במערכת יהלום.

1.3.2.4. פעולות במערכת ההזדהות הלאומית

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

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

~~1.3.2.1.1.~~1.3.2.4.3. בכל תקלה בהליך ההרשמה להזדהות הלאומית, או בתהליך ההזדהות יש לפנות למוקד התמיכה של המערכת (טלפון-1299, כתובת דואר אלקטרוני moked@mail.gov.il, טלפון נוסף 08-6863100).

1.3.2.4.4. פרטים נוספים על אודות הליך ההרשמה מפורטים בקישור זה.

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

1.3.2.5. פעולות במערכת יהלום

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

1.3.2.5.2. לאחר השלמת הגשת ההצעה במערכת תתקבל הודעה "הצעתך נשלחה בהצלחה" ומציע יוכל להוריד את מסמך ההצעה. מסמך ההצעה הוא מסמך חתום דיגיטלית של ההצעה ומהווה אסמכתה להצעה שהוגשה. המסמך ישלח לך למציע גם בדוא"ל. מסמך ההצעה האחרון שנשלח יוצג גם במערכת.

1.3.2.5.3. מציע יוכל לעדכן את הצעתו כל עוד לא חלף המועד האחרון להגשת הצעה.

1.3.2.5.4. ככל שלאחר שהוגשו הצעות בתיבה, ערך עורך המכרז שינוי במסמכי התיחור (למעט שינוי במועדי המכרז), הצעות שהיו בתיבה יבוטלו ויעברו למצב טיוטה ומציע המעוניין להגיש את הצעתו בהתאם לתנאי המכרז המעודכנים יידרש לבצע הגשה מחדש.

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

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

1.3.2.7.1. ניתן לעלות עד 10 קבצים כאשר גודל מקסימלי של כל קובץ (עד MB15).

1.3.2.7.2. פרק הזמן שבו המערכת מתנתקת בהיעדר פעולה של משתמש (20 דקות ל- time out).

1.3.2.7.3. מגבלות טכניות נוספות: על מנת להכיר את שאר מגבלות המערכת באחריות מגיש ההצעה לקרוא, מבעוד מועד, את המדריך להגשת הצעות באמצעות תיבת מכרזים דיגיטלית. בנוסף לרשותו של מגיש הצעה חומרי הדרכה אשר נועדו לסייע לו להגיש הצעות בהצלחה.

1.3.2.8. לסיוע טכני במקרה של תקלה או שאלה ניתן לפנות למוקד התמיכה בימים א'-ה' בין השעות 8:00-17:00 במייל: moked@mail.gov.il או באמצעות הצ'אט האנושי: https://mygovchat.gov.il/icr/bot.aspx?l=3.

1.3.2.9. בפניה יש לציין את שם המכרז, המועד האחרון להגשת ההצעות ובמידת הצורך לצרף צילומי מסך.

1.3.2.10. זמן ההמתנה מרגע משלוח הפניה ועד לחזרת נציג שירות לא יעלה על 4 שעות בטווח שעות פעילות המוקד.

1.3.2.11. מוקד התמיכה אינו מתחייב לספק מענה לפניות אשר יתקבלו בזמן קצר מ-4 שעות מהמועד האחרון להגשת הצעות.

1.3.2.12. מציע אשר מגיש את הצעתו כאשר נשארו פחות מ-4 שעות להגשת הצעות במכרז לוקח על עצמו את הסיכון שבמקרה של תקלה נציג השירות לא יספיק לפתור את הבעיה הטכנית שלו או לענות על שאלה שיש לו.

1.3.2.13. על מציע במכרז האחריות הבלעדית להגיש את ההצעה לפני המועד האחרון להגשת הצעות.

1.3.2.14. על המציע להביא בחשבון כי בסמוך למועד האחרון להגשת הצעות ייתכן עומס על מערכת ההגשה או תקלות טכניות אחרות אשר ימנעו מהמציע להגיש את הצעתו. על המציע להיערך לכך, ולהגיש את הצעתו מבעוד מועד.

~~1.3.2.2.~~1.3.2.15. למציע לא תהיה כל טענה למזמין באשר לתקלה שהתגלתה במערכת ההזדהות או במערכת הגשת ההצעות סמוך למועד האחרון להגשת הצעות, גם אם כתוצאה מכך הוא לא הצליח להגיש את הצעתו במכרז.

1.3.2.16. **ביטול אוטומטי של הצעה שהוגשה – תיקונים במסמכי המכרז**

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

1.3.2.16.2 ~~1.3.2.3.~~ באחריותו הבלעדית של המציע להתעדכן בסטאטוס הצעתו במערכת הגשת ההצעות.

~~1.3.2.4 מציע המעוניין להשתתף בתיחור יגיש את המענה שלו, כמפורט לעיל, לתיבת המכרזים הדיגיטלית, באמצעות מערכת הגשת הצעות מקוונת.~~

~~1.3.2.5 קישור למערכת הגשת ההצעות יפורסם לספקי המסגרת לפחות חמישה ימי עבודה טרם המועד האחרון להגשת הצעות.~~

~~1.3.2.6 המועד האחרון להגשת הצעות לתיבת המכרזים הדיגיטלית מפורט בנספח א' להלן.~~

~~1.3.2.7 לצורך הגשת הצעתו יידרש המציע להזדהות באמצעות מערכת ההזדהות הממשלתית ולבצע רישום מוקדם למערכת הגשת ההצעות.~~

~~1.3.2.8 לאחר ביצוע ההזדהות יש לוודא כי מופיעים במערכת להגשת ההצעות פרטי התיחור הרלוונטי.~~

~~1.3.2.9 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.~~

~~1.3.2.10 לאחר השלמת הגשת ההצעה במערכת יופיע במסך ההגשה מספר אסמכתהא. אם לא התקבל מספר אסמכתהא ההצעה לא הוגשה. בנוסף, עם השלמת ההגשה תשלח המערכת מייל עם נתוני ההצעה ובכלל זה כל הקבצים שהוגשו ושעת הגשתם, לכתובת המייל שהזין המשתמש במערכת. ניתן לאמת את פרטי ההצעה שהוגשה במערכת אל מול המייל או להיכנס בשנית לתיבה ולאמת את פרטי ההצעה אל מול הפרטים המופיעים בהצעה.~~

~~1.3.2.11 לא ניתן יהיה להגיש הצעות במערכת לאחר המועד האחרון להגשת הצעות.~~

~~1.3.2.12 **באפשרות המציע לבצע הגשה אחת בלבד**! לאחר השלמת הגשת הצעה לא תתאפשר הגשה נוספת או עדכון הצעה.~~

~~1.3.2.13 אם תהיה תקלה טכנית, אשר תמנע הגשת הצעות במכרז, יוכל עורך המכרז בהודעה שתפורסם לספקי המסגרת, לקבוע דרך הגשה אחרת במכרז.~~

~~1.3.2.14 תנאים נוספים לשימוש במערכת הגשת ההצעות:~~

~~1.3.2.14.1 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.~~

~~1.3.2.14.2. ניתן להעלות למערכת קבצים מסוג PDF / WORD / EXCEL.~~

~~1.3.2.14.3. קיימת מגבלה על מס' התווים בשם הקובץ שמועלה – 64 תווים לכל היותר.~~

~~1.3.2.14.4. סיוע טכני: בסוגיות טכניות ובעזרה בתפעול המערכת ניתן לפנות למוקד התמיכה בימים א'-ה' בין השעות 8:00 עד 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.~~

~~1.3.2.14.5. **בחלוף 20 דקות ללא ביצוע פעולה, המערכת תתנתק וכל פעולה שבוצעה בה ולא נשמרה כטיוטה, לא תשמר**. במקרה המתואר תידרש כניסה מחודשת למערכת. על מנת להכיר את שאר מגבלות המערכת באחריות מגיש ההצעה לקרוא את המדריך להגשת הצעות (קישור) מבעוד מועד. בנוסף לרשותו של מגיש הצעה חומרי הדרכה אשר נועדו לסייע לו להגיש את הצעות בהצלחה (קישור – https://portal.gpa.gov.il/supplier/tender).~~

~~1.3.2.14.6. להנחיות וחומרי הדרכה על אופן הגשת ההצעות בתיבת המכרזים הדיגיטלית ניתן להיכנס לקישור הבא: https://portal.gpa.gov.il/supplier/tender.~~

~~1.3.2.15. 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.~~

1.4. הליך בדיקת ההצעות

1.4.1. ההצעות לתיחור ייבחנו בהתאם לכללים המפורטים במסמכי המכרז המרכזי, בדגש על "חוברת מס' 2 למסמכי המכרז: הנחיות לגבי חלק ב' של המכרז" ("**חוברת מס' 2 למסמכי המכרז המרכזי**").

1.4.2. **שלב ראשון - חישוב ציון איכות**

1.4.2.1. לתיחור זה נקבע ציון איכות מינימלי, כמפורט בנספח 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.

1.4.2.2. 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: $\frac{72}{90} * 100 = 80$ נקודות

1.4.3. **שלב שני – חישוב מחיר משוקלל**

1.4.3.1. המציעים שהצעותיהם עמדו בתנאי הסף ובציון האיכות המינימלי, לפי העניין, יוזמנו להשתתף בשלב התיחור הדינאמי המקוון, במועד הרשום בנספח א'.

1.4.3.2. התיחור הדינאמי המקוון ייערך במערכת תיחורים חדשה – מערכת מיר"ב ("**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.

1.4.3.3. מועד ההדרכה על מערכת מירב יישלח בדוא"ל לכל ספקי המסגרת.

1.4.3.4. אופן הרישום ודגשים לשימוש במערכת מירב מפורטים בנספח ז'.

1.4.3.5. בתיחור הדינאמי המקוון יזין המציע כדלהלן:

1.4.3.5.1. אחוז הנחה ממחיר המחירון הרשמי לכלל המוצרים המוצעים על ידי המציע בתיחור.

1.4.3.5.2. עלויות עבור שירותי תחזוקה כמפורט בסעיפים הרלוונטיים בנספח ד' (עלות תחזוקה, עלות שעות עבודה וכו'), והכל בהתאם למפורט בנספח.

1.4.3.6. רכיבים אלו ישוקללו במהלך התיחור כמפורט במודל הייחוס (נספחים ד', ד'1).

1.4.3.7. המחיר המשוקלל של ההצעה בתיחור הדינאמי המקוון לא יעלה, בכל מקרה, על המחיר המירבי להצעה כפי שנקבע בהתאם לאמור בסעיף 1.4.5.4~~1.4.5.4~~ להלן.

1.4.3.8. 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.

1.4.3.9. המחיר הסופי לכלל המוצרים הרלוונטיים אצל היצרן יהיה מחיר המחירון הרשמי בניכוי אחוז ההנחה שניתן על ידי המציע למוצרים. יובהר כי המדורג ראשון בסיום התיחור יהיה רשאי להציע הצעת מחיר משופרת.

1.4.3.10. במקרה בו זכה המציע בשני תיחורים או יותר, וקיימים פריטים המשותפים לשני תיחורים או יותר, יקבע המחיר הנמוך מבין המחירים המוצעים למוצר.

1.4.3.11. 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.

1.4.4. **שלב שלישי - קביעת ציון מחיר**

1.4.4.1. מהמחיר המשוקלל של ההצעה ייגזר ציון המחיר בהתאם לנוסחה הבאה:

1.4.4.2. הגדרות:

TP_i – ציון המחיר של מציע i

p_i – המחיר המשוקלל של מציע i

$lowest\ price\ received$ – המחיר המשוקלל הנמוך ביותר שהתקבל על ידי מי מהמציעים.

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

$$TP_i = \left(1 - \frac{p_i - lowest\ price\ received}{Median\ price}\right) \times 100$$

1.4.5. **שלב רביעי - חישוב ציון ההצעה ודירוג ההצעות**

1.4.5.1. ציון המחיר ישוקלל יחד עם ציון האיכות המשוקלל של ההצעה בהתאם למפורט בסעיף 1.4.5.2~~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:

1.4.5.2. הגדרות:

G_i – ציון ההצעה של מציע i

Q_i – ציון האיכות המשוקלל של מציע i

TP_i – ציון המחיר של מציע i

W_q – משקל האיכות

W_p – משקל המחיר

$$G_i = W_p \times TP_i + W_q \times Q_i$$

1.4.5.3. להלן המשקלות בתיחור זה:

רכיב	משקל

משקל האיכות (W_q)	60%
משקל המחיר (W_p)	40%

1.4.5.4. **מחיר מירבי**

1.4.5.4.1. עורך המכרז יהיה רשאי, טרם ביצוע התיחור הדינאמי המקוון, לקבוע מחיר מירבי להצעה. במקרה זה המחיר המירבי יהיה זהה עבור כלל המציעים.

1.4.5.4.2. המחיר המירבי יועבר למציעים לפחות 7 ימי עבודה טרם מועד התיחור הדינאמי המקוון.

1.4.5.4.3. 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.

1.4.5.5. **תיחור מדמה**

1.4.5.5.1. תיחור מדמה ייערך בהתאם למפורט בסעיף 2.9.4 לנספח 2 לחוברת 2 למסמכי המכרז המרכזי.

1.4.5.5.2. התיחור המדמה יתקיים במועד המפורט בנספח א'.

1.4.5.5.3. ההשתתפות בתיחור המדמה הינה חובה ומהווה תנאי להשתתפות המציע בתיחור הדינאמי המקוון.

1.4.5.5.4. אם עורך 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.

1.4.6. **הצעה יחידה**

1.4.6.1. מבלי לגרוע מהאמור בסעיף 1.5.2 למסמכי המכרז המרכזי, אם הוגשה בתיחור הצעה יחידה, או שלאחר בדיקת ההצעות נותרה הצעה אחת בלבד, עורך המכרז, בהתאם לשיקול דעתו הבלעדי יהיה רשאי:

1.4.6.1.1. להכריז על המציע שנותר כזוכה;

1.4.6.1.2. לבטל את התיחור, ולצאת לתיחור חדש;

1.5. פרטי ההתקשרות

1.5.1. על ההתקשרות במסגרת תיחור זה יחולו הכללים המפורטים בפרק 3 למסמכי המכרז המרכזי – אופן ביצוע ומימוש ההתקשרות. להלן יפורטו תנאים ייחודיים לתיחור זה.

1.5.2. **<u>תקופת ההתקשרות</u>**

1.5.2.1. תקופת ההתקשרות מכוח התיחור ("**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.

1.5.2.2. 21 ימי העבודה הראשונים של תקופת ההתקשרות בתיחור יוגדרו כתקופת התארגנות, במהלכה הספק הזוכה יידרש להשלים היערכותו לקראת אספקת המוצרים והשירותים המבוקשים.

1.5.3. **<u>אחריות ותחזוקה</u>**

1.5.3.1. 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 <u>12 חודשים</u> מיום **הפעלת המוצר** (Activation), ואם המזמין רכש שירותי התקנה והטמעה, מיום אישור המזמין כי ההתקנה, אותה ביצע הספק בפועל, נעשתה לשביעות רצונו ובאופן הנדרש, לפי המאוחר ("**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.

1.5.3.2. הספק הזוכה יספק תקופות אחריות ותחזוקה נוספות, מעבר לתקופת האחריות הראשונה, בתעריף שהוצע על ידו במסגרת הצעתו בתיחור ולכל הפחות עד 36 חודשים ממועד תום תקופת ההתקשרות בתיחור ("**תקופת האחריות והתחזוקה**"). קרי, חובת האחריות והתחזוקה יכולה להימשך גם לאחר תום תקופת ההתקשרות.

1.5.3.3. 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.

1.5.3.4. **<u>הרחבת שירות לשירות 24/7</u>**

1.5.3.4.1. 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.

1.5.3.4.2. עבור הרחבת רמת שירות זו, תשולם לספק תוספת תמורה בהתאם למפורט להלן:

1.5.3.4.2.1. עבור מוצר או שירות ברכישה – תמורה בשיעור של <u>15% ממחיר התחזוקה השנתית</u> כפי שהוצעה בהצעתו – לדוגמה, עבור מוצר שעולה 5,000$, ועלות

האחריות והתחזוקה השנתית הינה 10% ממחיר הרכישה, תשלום 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=$500, תוספת התמורה עבור הרחבת השירות הינה 15%X500=75$).

1.5.3.4.2.2. 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$).

1.5.3.4.3. יובהר כי מזמין יוכל להפעיל ולהפסיק את הרחבת השירות בכל עת, כאשר הפסקת השירות תיכנס לתוקף במלאת שנה קלנדרית מהפעלת ההרחבה.

1.5.4. **<u>רישוי</u>**

1.5.4.1. 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.

1.5.4.2. הרישוי לצורך הקמת מעבדת בדיקה יהיה ללא עלות ויוגבל ל-30 יום.

1.5.4.3. על היצרן להחזיק ממשק ניהול רישיונות הניתן לגישת כלל המזמינים באמצעות רשת האינטרנט בו המזמין, לאחר זיהוי, יכול לקבל דיווח על כלל הרישיונות שרשומים בארגונו, תוקפם, תוקף הסכם התחזוקה וכדו'. 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.

1.5.4.4. עלות הרישוי בהקמת DR פאסיבי או להקמת "מערכת רדומה" (Active-Standby) יהיה 20% מעלות הרישוי כפי שנקבעה בתיחור.

1.5.5. **<u>התקנת והטמעת המוצרים והשירותים הנרכשים</u>**

1.5.5.1. המזמין רשאי לרכוש כחלק מהמוצרים והשירותים המבוקשים, גם שירותי התקנה והטמעה, וזאת בהתאם לאמור בסעיף 3.8.4 למסמכי המכרז המרכזי ולמפורט <u>בנספח ד'</u>.

1.5.5.2. אם המזמין 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 3.9.6-3.9.8 למסמכי המכרז המרכזי, ובהתאם למפורט להלן.

1.5.5.3. 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.

1.5.5.4. בנוסף, הספק יספק למזמינים מדריכים טכניים על המוצרים המסופקים. כמו כן, 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.

1.5.6. **התמורה עבור התקנת והטמעת המוצרים והשירותים הנרכשים**

1.5.6.1. עבור כל שעת התקנה והטמעה שבוצעה בפועל (**"שעת עבודה"**) יקבל הספק תמורה בסך של 250 ₪ (כולל מע"מ) לשעת עבודה.

1.5.6.2. התמורה עבור שעות עבודה שבוצעו מעבר לשעות העבודה המקובלות תהיה בכפוף לאמור בסעיף 3.8.4.4 למסמכי המכרז המרכזי.

1.5.6.3. 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 (**"מכרז שירותי מחשוב"**).

1.5.6.4. 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.

1.5.6.4.1. להלן דוגמה לאופן ביצוע ההצמדה: אם תעריף "מיישם הגנת סייבר ברמת התמחות ב' יעלה ל-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.

1.5.6.5. 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.

1.5.7. **צוות נותני השירותים**

1.5.7.1. בנוסף על האמור בסעיף 3.6.2.2.2 למסמכי המכרז, מזמין יהא רשאי, בהתאם לשיקול דעתו, לדרוש מהזוכה להחליף מיישם בכל עת ומכל סיבה סבירה, אשר תוצג בפני הספק הזוכה, והזוכה יקצה מיישם אחר במקומו עבור המזמין תוך 21 ימי עבודה.

1.5.8. **הוספת מוצרים ושירותים לרשימת המוצרים המאושרים לרכישה**

1.5.8.1. 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.

1.5.8.2. בנוסף לאמור לעיל, לעורך המכרז שמורה הזכות לאחר התיחור ובמהלך כל תקופת ההתקשרות בתיחור להוסיף לתכולת ההתקשרות מוצרים ושירותים שאינם בתחום מושא התיחור, אף אם הם אינם של יצרן ~~או ספק אחר מהזוכים בתיחור~~שמוצריו זכו בתיחור, ואשר נדרשים לצורך ייעול ומקסום השימוש בפריטים בתחום התיחור, בין היתר, מבין הקטגוריות:

1.5.8.2.1. התקנות, תחזוקה, שירות והדרכות נוספות.

1.5.8.2.2. אפליקציות ותוכנות מתממשקות.

1.5.8.2.3. חומרה להרצה מובנית של השירותים בתחום התיחור.

1.5.8.3. 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.

1.5.8.4. היקף הרכש של הפריטים שיתוספו במהלך תקופת ההתקשרות, לא יעלו במצטבר, על שיעור של 20% מהיקף הרכש שיתבצע מכוח התיחור.

1.5.9. **עיבוד ואבטחת מידע והגנה בסייבר בשירותים**

1.5.9.1. בנוסף על האמור במסמכי המכרז ובנספח ג' למסמך התיחור, מפורטים בנספח ח' כללים הנוגעים לאופן אספקת השירותים.

1.5.9.2. כללים אלו יחייבו את הספק והיצרן המוצע מטעמו ביחס לאספקת השירותים במסגרת התיחור.

1.5.10. **ערבות ביצוע**

1.5.10.1. 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.

1.5.10.2. הערבות תעמוד בתוקף עד ל-90 ימים מתום תקופת ההתקשרות בתיחור או תקופת האחריות והתחזוקה האחרונה, לפי המאוחר מביניהן.

2. נספח א' – פרטים כלליים לתיחור

2.1. מועדים בתיחור

מופע בתיחור	מועד
מועד אחרון להגשת שאלות הבהרה והערות	חלף
מועד אחרון להגשת שאלות הבהרה והערות סבב 2	~~21.1.2024~~חלף
פרסום עורך המכרז למענה לשאלות הבהרה	לפחות 12 ימים לפני המועד האחרון להגשת הצעות
מועד פתיחת תיבת המכרזים הדיגיטלית להגשת הצעות	20.3.2024 בשעה 12:00
מועד אחרון להגשת הצעות	10.4.2024 בשעה 14:00
תוקף הצעה לתיחור	~~9~~על פי סעיף 1.5.6 למסמכי המכרז תוקף ההצעה הוא 180 יום לאחר המועד האחרון להגשת ~~5.9.2024~~.
מועד תיחור מדמה (להצעות שעמדו בדרישות התיחור)	מועד התיחור המדמה יישלח בנפרד
מועד תיחור דינאמי מקוון (להצעות שעמדו בדרישות התיחור)	מועד התיחור הדינאמי יישלח בנפרד

2.1.1. מועדים אלו הינם לידיעה בלבד ואינם מהווים אישור לתקינות ההצעה ולהשתתפות בתיחור הדינאמי המקוון.

2.1.2. השתתפות מציע בתיחור הדינאמי המקוון מותנית בהודעת ועדת המכרזים על אישור הצעתו להשתתפות בתיחור.

2.1.3. תוקף ההצעה רשום בטבלת התאריכים לעיל. עורך המכרז רשאי להודיע על הארכת תוקף ההצעה לתקופה נוספת של עד ~~90~~ 180 ימים (ובהסכמת ספק המסגרת אף מעבר לכך), זאת עד לבחירת זוכה. המציע אינו רשאי לחזור בו מהצעתו בתקופה האמורה.

2.2. ציון איכות מינימלי ומשקלות למתן ציון

2.2.1. 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%.

2.2.2. להלן יפורטו המשקלות לצורך מתן ציון האיכות:

מס"ד	נושא	משקל	ציון איכות מינימלי
1.	הערכת קו המוצרים המוצע (היקף המערכת המוצעת, יכולות המערכת,	40%	

	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 וכדו׳).		
.2	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 וכדו׳).	15%	85%
.3	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 וכדו׳).	10%	
.4	הערכת היקף ויכולת מרכז הפיתוח בארץ (במקרה של התחייבות היצרן להקמת מרכז כאמור במקרה של זכייה במכרז, יינתן ניקוד חלקי).	15%	
.5	הערכת יכולת המציע (ניסיון בתחום ובתחומים דומים, מס׳ עובדים בתחום, הכשרות רלוונטיות וכדו׳).	20%	
	סה״כ	100%	**80%** (למעט רכיב ״הערכת היקף ויכולת מרכז פיתוח בארץ״)

3. 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 המרכזי 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
____________	____________	____________	____________
____________	____________	____________	____________

(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

4.1. הנחיות למענה על נספח זה

4.1.1. סעיפים בהם קיימת דרישה מפורשת לתכונה או יכולת, **הינם סעיפי חובה**, ולא תתקבל הצעה שאינה כוללת מענה לדרישה או ליכולת המפורטת בסעיף. אם בסעיף נדרש פירוט לגבי אופן המענה, על המציע לספק פירוט כנדרש.

4.1.1.1. אלא אם נקבע אחרת בסעיף ספציפי, המערכת המוצעת נדרשת לעמוד בכל סעיפי החובה המפורטים בנספח זה, **נכון למועד האחרון להגשת הצעות בתיחור.**

~~4.1.1.~~4.1.2. 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.

~~4.1.1.1.~~4.1.2.1. אם סעיפים אלו אינם מתקיימים בפתרון המוצע במועד האחרון להגשת הצעות, אך יש צפי לקיומם, יש לציין לוח זמנים.

~~4.1.2.1.1.1. סעיפים בהם קיימת דרישה מפורשת לתכונה או יכולת, **הינם סעיפי חובה**, ולא תתקבל הצעה שאינה כוללת מענה לדרישה או ליכולת המפורטת בסעיף. אם בסעיף נדרש פירוט לגבי אופן המענה, על המציע לספק פירוט כנדרש.~~

~~4.1.2.1.1.1.1.1. אלא אם נקבע אחרת בסעיף ספציפי, המערכת המוצעת נדרשת לעמוד בכל סעיפי החובה המפורטים בנספח זה, **נכון למועד האחרון להגשת הצעות בתיחור.**~~

4.1.2.2. על אף האמור בסעיף 2.3.4 למסמכי המכרז המרכזי (נספח חוברת הנחיות לתיחורים), אם עורך המכרז סבור כי היקף ההשלמות הנדרש ביחס להצעה מסוימת, מהותי מבחינת היקף העבודה ומשך הזמן הנדרשים לצורך בקשת השלמות ובדיקתן, לא תתבצע פנייה להשלמות.

4.1.3. **יובהר כי, כל הסעיפים המפורטים בנספח ג׳**, קרי סעיפי החובה וסעיפי הפירוט (איכות) **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.

4.1.4. **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.**

4.1.5. מענה לנספח זה ניתן להגיש הן בשפה העברית והן בשפה האנגלית.

4.2. תנאים ודרישות לגבי היצרן והמציע

4.2.1. בנוסף לקיום מוקד שירות פעיל ע״י המציע כמפורט בסעיף 3.13.6.2 למסמכי המכרז המרכזי, היצרן יידרש לספק מרכז תמיכה שישמש כתובת לפניות ושאלות מקצועיות (״**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.

4.2.2. מרכז התמיכה נדרש לספק תמיכה בשפה האנגלית. נדרש פירוט לגבי יכולת תמיכה בשפה העברית.

4.2.3. הזוכה יידרש לספק מסמכי המלצת יצרן (Best Practices) להגדרות הגנה מומלצות מטעמו בתחום ה-SSE על בסיס מתודולוגיות ~~מ~~מקובלות, לרבות ביחס לאופן השימוש במוצר על מנת להגיע לסטנדרט אבטחה מקובל כדוגמת ISO-27002 ו-NIST.

4.2.4. 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 במוצריו, לרבות פרק הזמן לדיווח על כך.

4.2.5. **מקום פיתוח המוצר:**

4.2.5.1. על המציע לפרט את מיקום פיתוח המוצרים בתחום מושא התיחור. יש לצרף אישור יצרן בהתאם.

4.2.5.2. אם היצרן מתחייב להקים מרכז פיתוח בארץ בתחום מושא התיחור, יש לספק פירוט על כך ולצרף התחייבות של היצרן בהתאם.

4.2.6. **פרטים לגבי ניסיון המציע במוצר המוצע:**

4.2.6.1. נדרש פירוט על ניסיון המציע במוצר המוצע, לרבות שנת התחלת העבודה עם היצרן המוצע, רמת ההסמכה של המציע מטעם יצרן המערכת המוצעת וכל מידע אחר רלוונטי.

4.2.6.2. נדרש פירוט של כלל המיישמים המועסקים מטעם המציע להם הסמכה של היצרן למוצרים והשירותים המוצעים בתיחור לפי הפורמט הבא:

מס'	שם העובד	שנות ניסיון בתחום התיחור	ההסמכה למוצרים המוצעים	שנת קבלת ההסמכה	סיווג בטחוני אם ישנו
1					
2					
3					
4					
5					

~~4.2.7. למציע מוקד שירות פעיל כמפורט בסעיף 3.13.6.2. למסמכי המכרז המרכזי.~~

~~4.2.8.~~4.2.7. על המציע לספק פירוט לגבי אופן התמיכה שלו בשירותים המפורטים להלן:

~~4.2.8.1.~~4.2.7.1. מתן ייעוץ וסיוע בהגדרת הפתרון המוצע אצל המזמינים – יש לפרט את אופי השירותים המוצעים.

4.2.8.2 4.2.7.2 מתן עזרה באתר המזמין – יש לפרט את תהליכי הסיוע והאסקלציה.

4.2.8.3 4.2.7.3 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.

4.3. דרישות מהמערכת/מוצרים

4.3.1. שירותי **Secure Service Edge (SSE)** לעניין תיחור זה הם כלל הכלים והטכנולוגיות (כולל **Secure Web Gateway (SWG)**, **Zero Trust Network Access (ZTNA)** ו- **Cloud Access Security Broker (CASB)**) המשמשים כפלטפורמה לצמצום הסיכונים לאובדן מידע ומניעת גישת בלתי מורשים למשאבים מקומיים, מבוססי-ענן ומקוונים תוך מתן יכולות ניהול, שליטה ואכיפת מדיניות, הגנה על נכסי מידע וצמצום אירועים של פגיעה במידע.

4.3.2. המערכת והרישיונות המוצעים במודל הייחוס יכללו את כלל הדרישות המפורטות בנספח זה, ללא תוספת תשלום, כולל כלל רכיבי הענן הנדרשים להפעלת המוצרים והשירותים המבוקשים וכן יכולות התממשקות למוצרי הצד השלישי הנדרשים במסמכי התיחור.

4.3.3. 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 כ מידע או חשש מהפסקת מכירה, ייצור, אספקה או תמיכה של המוצרים והשירותים (או רכיבים או פריטים המשמשים אותם) המוצעים על ידו.

4.3.4. יש לוודא כי הצעת המציע לכל אחד מהרכיבים הנדרשים במודל הייחוס (סעיף 4.3.7 4.3.7) כוללת את כל הרישוי הנדרש להפעלת המערכת והשימוש בה.

4.3.5. יש לצרף מפרט רישוי ברור ומובן לכל רכיב מוצע בהתאם למודל הייחוס, וכן לציין את מודל הרישוי (Perpetual, Subscription וכו').

4.3.6. יש לצרף מסמך Best Practice של היצרן בנוגע לניהול ואופטימיזציה של הרישיונות ותפעולם.

4.3.7. **להלן פירוט המוצרים הנדרשים:**

4.3.7.1. **שירותי SSE תוכנתי בענן (SaaS):**

נושא	מענה המציע	הערות
רישיון SSE, תמיכה ב-50,000 רישיונות.		יש לפרט את כלל המוצרים המסופקים בהצעת המציע לרבות מערכת הניהול ורכיבי שרידות המערכת.
מערכת ניהול התומכת ב-50,000 רישיונות, לרבות שרידות, עם תמיכה בניהול Multitenant.		
פירוט החומרה הנדרשת להתקנת מערכת הניהול (לרבות שרידות).		~~כמות זו, היא כמות מוערכת לכלל המזמינים.~~

		נא תשומת לבבם לסעיף 5.5.15.5.1 בנספח ד' להלן.

.4.4 דרישות טכנולוגיות

.4.4.1 דרישות תצורה

.4.4.1.1 המענה נדרש לכלול פתרון SSE בענן (SaaS) בפלטפורמה של יצרן יחיד, בהתאם לדרישות המפורטות בסעיף 4.4.114.4.5.10 להלן. נדרש פירוט לגבי אופן מימוש תצורת פריסה זו.

.4.4.1.2 תצורות פריסה נוספות:

.4.4.1.2.1 נדרש פירוט לגבי תמיכת המערכת בתצורת התקנה 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.

.4.4.1.2.2 נדרש פירוט לגבי תמיכת המערכת בתצורה היברידית הכוללת שילוב של רכיבים מקומיים ועננים.

.4.4.1.3 נדרשת תמיכה ביכולת שרידות ללא פגיעה בפעילות משתמשי הקצה. יש לפרט את אופן מימוש הדרישה.

.4.4.1.4 נדרש כי הפתרון יתמוך בתצורת DR למקרה כשל. נדרש פירוט לגבי אופן מימוש ה DR ודרישות טכנולוגיות למימוש.

~~נדרשת תמיכה בהטמעת המערכת באתר DR.~~

.4.4.1.5 נדרשת תמיכת המערכת בתצורת High Availability (HA) ויתירות תקשורת ואספקת מתח.

~~.4.4.1.3~~.4.4.1.6 נדרש פירוט לגבי התממשקות לכלים ופלטפורמות שונות, לרבות Microsoft SQL DB ו-Windows Server 2016 ומעלה, יכולת הטמעת רכיבים בתצורת Image כגון OVA (Linux). יש לפרט פלטפורמות וכלים נוספים אותם ניתן לממשק למערכת.

.4.4.2 ארכיטקטורה מרכזית לתפעול וליישום מדיניות ניהול ואכיפה

.4.4.2.1 נדרשת יכולת ניהול ב-Multi-Tenant בהרשאות מוגדרות למערכת ניהול הרישיונות, בעבור גדלי משרדים שונים, בפתרון ענן ממשלתי פרטי וציבורי.

~~.4.4.2.2 נדרשת יכולת הטמעה בארכיטקטורת High Availability~~

~~.4.4.2.3~~.4.4.2.2 נדרשת יכולת ניהול מ-Console ניהול מרכזי.

.4.4.3 SWG – גישה מאובטחת לתשתיות Web, Cloud

.4.4.3.1 פריסת המערכת

~~.4.4.3.1.1 נדרש כי המציע יעמיד בסיס תמיכה מקומי/ישראלי במוצר המוצע ובפריסתו;~~

~~כמפורט במסמכי המכרז והתיחור.~~

~~4.4.3.1.2.~~4.4.3.1.1 נדרשת תמיכה ביכולות הבאות תוך ניהול ממשק מרכזי אחוד:

~~4.4.3.1.2.1.~~4.4.3.1.1.1 Proxy (~~Cache &~~ Authentication)

~~4.4.3.1.2.2.~~4.4.3.1.1.2 .Anti-Malware

~~4.4.3.1.2.3.~~4.4.3.1.1.3 URL Filtering.

~~4.4.3.1.2.4.~~4.4.3.1.1.4 .SSL Termination/Inspection

~~4.4.3.1.2.5.~~4.4.3.1.1.5 .Protocol Filtering (Application Filtering)

~~4.4.3.1.2.6.~~4.4.3.1.1.6 .Reporting

~~4.4.3.1.2.7.~~4.4.3.1.1.7 נדרש פירוט לגבי תמיכה ביכולות נוספות כגון Quota enforcement ו-CDR Integration.

~~4.4.3.1.2.8.~~4.4.3.1.1.8 נדרש פירוט על אופן האינטגרציה לרכיב ה-CASB המוצע, כמפורט בסעיף 4.4.5~~4.4.5~~ להלן.

4.4.3.2. נדרש כי המוצר יתמוך בתעבורת ~~IPV6,~~ NTP, DNS.

~~4.4.3.3. נדרשת תמיכת המערכת בתצורת (HA) High Availability ויתירות תקשורת ואספקת מתח. יש לפרט איך המערכת עונה על דרישה זו.~~

~~4.4.3.4.~~4.4.3.3 נדרש פירוט על תמיכה במנגנון המאפשר חסימה מיידית של כלל התקשורת לרשת האינטרנט לשימוש במקרה של התפרצות קוד זדוני ו/או ניסיון פריצה (כגון Panic Button).

~~4.4.3.5.~~4.4.3.4 נדרש כי הפתרון יתמוך בעבודה עם מספר סגמנטים ובניטור תעבורה ממספר סגמנטים כדוגמת: DMZ ,WAN, Wi-Fi.

~~4.4.3.6.~~4.4.3.5 נדרש כי מערך הניהול יאפשר גישה בשילוב עם מנגנוני הזדהות חזקה MFA.

~~4.4.3.7.~~4.4.3.6 נדרש פירוט על יכולת אינטגרציה של המוצר למערכות אבטחה אחרות, כגון DLP, IPS ואחרות.~~.~~ נדרש פירוט לגבי המערכות הנתמכות סוגי ומאפייני האינטגרציה למערכות צד ג'.

~~4.4.3.8.~~4.4.3.7 נדרש כי המוצר יאפשר חיפוש מאובטח על בסיס מנועי המערכת (Application URL Categorization,Blocking ועוד).

~~4.4.3.9.~~4.4.3.8 נדרש פירוט לגבי יכולת בניית חוקה על בסיס מיקום גאוגרפי או שעות פעילות.

~~4.4.3.10.~~4.4.3.9 נדרש כי מנגנון הדיווח על הפרת החוקה יכלול בין היתר את הפרמטרים הבאים:

~~4.4.3.10.1.~~4.4.3.9.1 שם המשתמש.

~~4.4.3.10.2.~~4.4.3.9.2 כתובת IP.

~~4.4.3.10.3.~~4.4.3.9.3 החוק שהופר.

~~4.4.3.11.~~4.4.3.10 נדרש כי ניהול מדיניות משתמשים מחוץ לארגון ומשתמשים במשרדי הארגון ינוהלו מפלטפורמת ניהול מרכזית.

4.4.3.11~~4.4.3.12.~~ נדרש פירוט לגבי יכולת הגבלת משתמשים מהורדת כמות מסוימת של נתונים מוגדרת, ולדוגמא, הגבלת המשתמש להורדה של לא יותר מ-GB 1 במהלך מרווח זמן קבוע.

4.4.3.12~~4.4.3.13.~~ נדרש כי הפתרון יאפשר קביעת מועד מוגדר לגיבוי הגדרות המערכת. נדרש פירוט לגבי אופן הגיבוי ודרישות נוספות.

4.4.3.13~~4.4.3.14.~~ נדרש כי הפתרון יתמוך בארכיטקטורת ניהול ובממשק משתמש מרכזי מבוסס Web הכולל יכולת ניטור, דיווח, תחזוקה והפעלת חוקה ומדיניות.

4.4.3.14~~4.4.3.15.~~ נדרש כי ממשק ניהול המערכת יתאפשר באמצעות פרוטוקולי גישה מוצפנים המבוססים על פרוטוקולים עדכניים כגון HTTPS, SSH.

4.4.3.15~~4.4.3.16.~~ נדרש כי הפתרון יתמוך בניהול מבוסס RBAC. יש לפרט לגבי פרופילי גישה default במערכת וכמו כן לגבי יכולת התאמה ובניית פרופילים חדשים.

4.4.3.16~~4.4.3.17.~~ נדרש כי הפתרון יתמוך ביכולות הכנסת אובייקטים כגון משתמש, כתובות IP, כתובות אתרים ודומיינים לרשימה שחורה או רשימה לבנה.

4.4.3.17~~4.4.3.18.~~ נדרש כי המערכת תאפשר הגבלת משתמשים מהורדת סוגי קבצים שונים על בסיס Extension. נדרש פירוט לגבי יכולות חסימה נוספות כגון True File Type.

4.4.3.18~~4.4.3.19.~~ נדרש כי המערכת תאפשר יכולת סינון וחסימת קטגוריות מוגדרות מראש כגון רשתות חברתיות. כמו כן נדרש כי למערכת תהיה יכולת הגבלה פנים אפליקטיבית כגון חסימת יכול צ'ט או וידאו בתוך רשת חברתית כגון Facebook.

4.4.3.19~~4.4.3.20.~~ נדרש פירוט לגבי תמיכה ביכולת בידוד גלישה (Remote Browser Isolation (RBI)). נדרש פירוט לגבי יכולת בידוד על בסיס משתמשים, קבוצות ויכולות בידוד נוספות. ככל שקיימת תמיכה ביכולת RBI, נדרש פירוט לגבי תמיכה בניהול מממשק מרכזי אחוד, ללא צורך לתפעל מוצרים נפרדים.

4.4.3.20~~4.4.3.21.~~ נדרש פירוט לגבי יכולות אימות משתמשים/קבוצות, לרבות בתצורות הבאות: Windows Authentication (Kerberos), NTLM v1 and v2 in Session Security, LDAP.

4.4.3.21~~4.4.3.22.~~ נדרש פירוט לגבי יכולת הפתרון לתמוך בפרמטר XFF (X-Forward For) לזיהוי כתובת לקוח מקורית. נדרש פירוט לגבי יכולות זיהוי נוספות.

4.4.3.22~~4.4.3.23.~~ נדרש פירוט לגבי יכולת שליחת התראות למשתמשים מוגדרים באמצעות דואר אלקטרוני וSMS. פירוט לגבי אפשרויות נוספות להעברת התראות.

4.4.3.23~~4.4.3.24.~~ נדרש כי הפתרון יאפשר עדכוני איומים בזמן אמת, עדכוני חתימות וכתובות אתרים זדוניים, אתרי פורנו, אתרי טרור, אתרים מבוססי דת, אתרי הימורים, אתרי תקיפה, אתרי פרוקסי ואנונימיזציה, פקודות תוכנות זדוניות, אתרי C&C, רשתות בוטים, מסדי נתונים לזיהוי תוכנות כופר והונאות אחרות.

4.4.3.24~~4.4.3.25.~~ נדרש פירוט לגבי יכולת תזמון ואופי עדכוני מנועים וDB המערכת.

4.4.3.25~~4.4.3.26.~~ נדרש פירוט לגבי תמיכה בפרוטוקולים כגון SNMPv2c, V3 ומעלה.

4.4.3.27.4.4.3.26. נדרש כי הפתרון יתמוך ב-Binding. נדרש פירוט על תמיכה ב-Binding על בסיס: User, IP, MAC.

4.4.3.28.4.4.3.27. נדרש פירוט לגבי תמיכה ב out time session וב-Idle Time out לאכיפת ניתוק המשתמשים.

4.4.3.29.4.4.3.28. נדרש פירוט לגבי תמיכה בסריקת פרוטוקול FTP Over HTTP.

4.4.3.30.4.4.3.29. נדרש כי הפתרון יאפשר חסימת דפים המכילים:

4.4.3.30.1.4.4.3.29.1. Malicious JavaScript / VB Script.

4.4.3.30.2.4.4.3.29.2. Malicious (or unauthorized) ActiveX applications.

4.4.3.30.3.4.4.3.29.3. Block Potentially Unwanted Programs (PUPs).

4.4.3.30.4.4.4.3.29.4. Malicious Windows executables.

4.4.3.31.4.4.3.30. נדרש כי הפתרון יתמוך בסריקת סוגים שונים של קבצים דחוסים (Nested Compressed Files).

4.4.3.32.4.4.3.31. נדרש פירוט לגבי תמיכת הפתרון המוצע ב- Caching, לרבות יכולות ונפחי הCache המוצעים בפתרון וכמו כן פירוט בנוגע ל-Latency.

4.4.3.33.4.4.3.32. נדרש כי המוצר יאפשר שימוש ב Web Proxy auto discovery protocol על מנת לאפשר למנהלי המערכת הגדרת מדיניות וProxy דינאמי למשתמשים (Auto proxy configuration in the browser).

4.4.3.34.4.4.3.33. נדרש כי המוצר יאפשר ניטור וחסימת תוכנות מסרים מידיים והעברת קבצים על גבי תוכנות אלה.

~~4.4.3.35. נדרש כי הפתרון יתמוך בתצורת DR למקרה כשל. נדרש פירוט לגבי אופן מימוש ה DRודרישות טכנולוגיות למימוש.~~

4.4.3.34. נדרש כי הפתרון יהיה ניתן להרחבת רישיונות ללא צורך בDowntime.

4.4.3.35. נדרשת תמיכה בהגנה מפני מתקפות Zero Day למשתמשים בנדידה.

4.4.3.36. נדרשת תמיכה בהגנה מפני ניצול פגיעויות על גבי דפדפנים (כדוגמת HTML Smuggling). נדרש פירוט לגבי אופן היישום, מנועי סריקה ויכולות נוספות בנושא זה.

~~נדרשת יכולת SSL Inspection למשתמשים מקומיים ולמשתמשים בנדידה.~~

4.4.3.37. נדרש פירוט לגבי יכולת הגדרת אישור או חסימת תעודות בלתי מוכרות (Untrusted Certificates).

4.4.3.38. נדרשת יכולת גישה למסדי נתונים מקוונים ואו מקומיים לקטלוג URL's כזדוניים, מאושרים. נדרש פירוט לגבי יכולות ~~SSL Inspection~~, חסימה, ניטור הHostname/IP address על בסיס נתוני ערך הסיכון (Risk Score).

4.4.3.39. נדרש פירוט לגבי כמות הקטגוריות הנתמכות על ידי מודול הגישה המאובטחת ל Web. נדרש פירוט לגבי כמות הקטגוריות אליהן יכולה להיות משויכת כתובת URL. נדרש פירוט לגבי יכולות קביעת

החוקה על בסיס קטגוריות אלה.

4.4.3.40. נדרשת תמיכה ביצירת קטגוריה מותאמת אישית וצירוף כתובות URL באופן ידני לקטגוריה.

4.4.3.41. נדרשת יכולת הגדרת מדיניות על בסיס קטגוריות מוגדרות מראש ומותאמות אישית כגון שיתוף קבצים, הימורים ועוד.

4.4.3.42. נדרשת תמיכה בפרוטוקולים הבאים:

~~TLS1.3.~~

4.4.3.42.1. HTTP/3.

4.4.3.42.2. HTTPS.

4.4.3.42.3. DoH.

4.4.3.42.4. IPv6.

4.4.3.43. נדרשת תמיכה בהצפנה מלאה בין הClient לשרתי ה Proxy. נדרש פירוט לגבי אופן התמיכה ~~בפרוטוקול~~ ופרוטוקולי ההצפנה הנתמכים ~~נוספים~~.

4.4.3.44. נדרשת תמיכה בזיהוי פגיעויות (Malware Detection) על בסיס חתימות (Signatures). נדרש פירוט לגבי תמיכה בזיהוי על גבי מכשיר המשתמש.

4.4.3.45. נדרש פירוט לגבי מנועי Sandbox מוטמעים.

4.4.3.46. נדרש פירוט על ~~ת~~ תמיכה בזיהוי פעילות זדונית או פעילות צל טכנולוגית (Shadow IT). נדרש פירוט לגבי אופן ויכולות הזיהוי.

4.4.3.47. נדרשת תמיכה ביכולת עריכת דפים חסומים.

4.4.3.48. נדרש פירוט בנוגע לתמיכה ביכולת אכיפת מדיניות גם כאשר יחידת הקצה איננה מקוונת.

~~4.4.3.36.~~ 4.4.3.49. SSL

~~4.4.3.36.1.~~ 4.4.3.49.1. נדרש כי הפתרון יסרוק תעבורת Traffic, SSL, https ויספק פענוח תעבורה מוצפנת ויכולת הצפנתה מחדש.

~~4.4.3.36.2.~~ 4.4.3.49.2. נדרש פירוט לגבי יכולת הפתרון לייבא Server Side Certificate ומפתחות פרטיים לפתיחת הצפנה.

~~4.4.3.36.3.~~ 4.4.3.49.3. הפתרון נדרש לתמוך בפרוטוקולי ההצפנה הבאים TLS 1.2, SSLv3, and SSLv2.

~~4.4.3.36.4.~~ 4.4.3.49.4. נדרשת תמיכה באלגוריתמים הבאים RSA, DHE, ECDHE וכמו כן MD5, SHA-1, SHA-256 hash.

~~4.4.3.36.5.~~ 4.4.3.49.5. נדרש פירוט לגבי תמיכה בשיטות נוספות כגון AES 3DES, DES, RC4, Camellia.

~~4.4.3.36.6.~~ 4.4.3.49.6. נדרש פירוט לגבי תמיכה בתעודות X.509.

4.4.3.36.7.4.4.3.49.7 נדרש פירוט לגבי תמיכה ב CA קיים ובמנגנון PKI קיים בארגון כולל ביצוע פעולות כגון Revocation Management.

4.4.3.36.8.4.4.3.49.8 נדרש פירוט לגבי תמיכה במערך HSM.

4.4.3.36.9.4.4.3.49.9 נדרש פירוט לגבי תמיכה בפרוטוקול OCSP stapling.

4.4.3.37.4.4.3.50 מנועי המערכת

4.4.3.37.1.4.4.3.50.1 נדרשת תמיכה ביכולות זיהוי וחסימת פוגענים מובנית ומנוהלת מרכזית דרך הממשק המערכתי.

4.4.3.37.2.4.4.3.50.2 נדרש כי הפתרון יספק ראיות פורנזיות בעת זיהוי פוגען ברשת ובין היתר:

4.4.3.37.2.1.4.4.3.50.2.1 Event timestamp.

4.4.3.37.2.2.4.4.3.50.2.2 Network events in sequence.

4.4.3.37.2.3.4.4.3.50.2.3 Malware behaviors.

4.4.3.37.2.4.4.4.3.50.2.4 Malware type.

4.4.3.37.2.5.4.4.3.50.2.5 Source and destination of attack.

4.4.3.37.2.6.4.4.3.50.2.6 נדרש פירוט לגבי תמיכה בפרמטרים נוספים כגון Packet capture of suspicious communication, Severity by malware type וכו'.

4.4.3.37.3.4.4.3.50.3 נדרשת תמיכה בפתרון זיהוי פוגענים המורכב ממספר מנועים וכולל בין היתר יכולות זיהוי מבוססות חתימות ויכולות זיהוי שאיננה מבוססת חתימות(Signature and Heuristics based).

4.4.3.37.4.4.4.3.50.4 כמו כן נדרשת תמיכה בזיהוי פוגענים מוטמנים בתוך קבצים כגון PDF (Embedded Files).

4.4.3.37.5.4.4.3.50.5 נדרשת תמיכה ביכולת בניית מדיניות אבטחה על בסיס פרוטוקולים שונים. נדרש פירוט על היקף התמיכה, לרבות ביכולת הגדרת מדיניות על בסיס פרמטרים שונים כגון אישור פעולה, חסימת פעולה, ניטור, הגדרת זמני שימוש, הגדרת נפחים מורשים.

4.4.3.37.6.4.4.3.50.6 וכמו כן נדרשת יכולת זיהוי אירועים על בסיס הקטגוריות הבאות לכל הפחות:

4.4.3.37.6.1.4.4.3.50.6.1 Advanced Malware Command and Control category.

4.4.3.37.6.2.4.4.3.50.6.2 Advanced Malware payload detection category.

4.4.3.37.6.3.4.4.3.50.6.3 Malicious embedded links and iframe detection category Mobile malware category.

4.4.3.37.6.4.4.4.3.50.6.4 Key logger and Spyware category.

4.4.3.37.6.5.4.4.3.50.6.5 P2P software category.

4.4.4. **Zero Trust Network Access ,Private Access**

4.4.4.1. נדרש פירוט לגבי אופן החיבור של משתמשים חיצוניים למערכת.

4.4.4.2. נדרשת תמיכה בהגדרת Watch list לניטור משתמשים נבחרים המזהים התנהגות חשודה.

4.4.4.1.1.

4.4.4.2.4.4.4.3. נדרש פירוט לגבי יכולות המוצר לספק יכולות בדיקה ברמות השונות ובין היתר:

4.4.4.2.1.4.4.4.3.1 Network Level.

4.4.4.2.2.4.4.4.3.2 Context Aware.

4.4.4.2.3.4.4.4.3.3 Identity Based Access.

4.4.4.3.4.4.4.4. נדרש פירוט לגבי האופן בו המוצר מצמצם את העלויות הכרוכות בIT ובתקשורת.

4.4.4.4.4.4.4.5. נדרש פירוט לגבי הגנה מפני איומים על גבי תעבורת ה ZTNA.

4.4.4.5.4.4.4.6. נדרש פירוט לגבי יכולת המערכת לייעל תהליכים כגון ניתוב, והשהיה (Latency).

4.4.4.6.4.4.4.7. נדרש פירוט לגבי תמיכה במערכות הפעלה ובין היתרן:

4.4.4.6.1.4.4.4.7.1 Windows.

4.4.4.6.2.4.4.4.7.2 Mac.

4.4.4.6.3.4.4.4.7.3 Linux.

4.4.4.6.4.4.4.4.7.4 iOS.

4.4.4.6.5.4.4.4.7.5 Android.

4.4.4.7.4.4.4.8. נדרשת תמיכה בזיהוי רכיבים מנוהלים ובלתי מנוהלים.

4.4.4.8.4.4.4.9. נדרשת תמיכה ביכולות חסימה והתראה על בסיס Geolocation. נדרש פירוט בנוגע ליכולת יצירת חוקה ומדיניות על בסיס Geolocation Information.

4.4.4.9.4.4.4.10. נדרש פירוט לגבי תמיכה ביצרני שירותי SaaS או ענן עימם קיימים הסכמי המאפשרים טיוב התעבורה.

4.4.4.10.4.4.4.11. נדרש פירוט בנוגע לאינטגרציה עם טכנולוגיות וספקיות SD-WAN.

4.4.5. **מודול ניהול ואבטחת מידע למערכות ענן (CASB)**

4.4.5.1. כללי

4.4.5.1.1. נדרשת יכולת מעקב אחר שינויים במדיניות ובהגדרות שירותי הענן המנוטרים, כולל נדרש פירוט לגבי יכולת ביצוע Roll Back.

4.4.5.1.2. נדרש פירוט לגבי יכולת בדיקת המדיניות טרום החלתה על גבי הסביבה הארגונית.

4.4.5.1.3. נדרש פירוט לגבי היכולת לספק מערכת להטמעה בסביבת בדיקות.

4.4.5.1.4. נדרשת תמיכה בחשיפת מידע (Metadata) באשר לשירות הענן אליו קיימת גישה למשתמשי הארגון:

4.4.5.1.4.1. פונקציונליות (כגון: מדיה חברתית, שיתוף קבצים).

4.4.5.1.4.2. האזור ממנו מסופק שירות הענן.

4.4.5.1.4.3. נקודות תורפה ידועות של שירות הענן.

4.4.5.1.5. ~~חישוב הסיכון הכללי עבור שירות הענן,~~ נדרש פירוט לגבי יכולת הצגת חישוב סיכון כללי עבור שירות ענן. נדרש פירוט על יכולת המשתמש לצפות בפרמטרים אשר הובילו לחישוב הסיכון.

4.4.5.1.6. נדרש פירוט לגבי מדיניות הצפנה לנתונים המאוכסנים בשירות הענן.

4.4.5.1.7. נדרש פירוט לגבי פרוטוקולי הצפנה המשמשים להעברת נתונים בשירות הענן.

4.4.5.1.8. נדרשת תמיכה בהערכת ציות שירותי הענן אל מול התקינות/רגולציות הבאות:

4.4.5.1.8.1. GDPR.

4.4.5.1.8.2. PCI.

4.4.5.1.8.3. ISO.

4.4.5.1.8.4. HIPAA.

4.4.5.1.9. נדרש פירוט לגבי תמיכה בתקינה או רגולציה נוספת, כדוגמת CSA.

4.4.5.1.10. נדרש פירוט לגבי תמיכה, בכל מקרה של פרצת אבטחה אצל ספק שירותי ענן, בדיווח אשר כולל פרטי הפריצה ומידע על שימוש העובדים בשירות הענן הנפרץ.

4.4.5.1.11. נדרש פירוט לגבי יכולות מניעת דלף מידע. נדרש פירוט לגבי מאפיינים לפונקציונליות זאת תוך שימוש ובהיעדר שימוש בסוכן.

4.4.5.1.12. נדרש פירוט לגבי תמיכה להגדרת התראה כ False Positive או כ False Negative לצורך טיוב מנוע הסיכונים.

~~4.4.5.1.3.~~4.4.5.1.13. נדרשת תמיכה בקבצי לוגים ממקורות Gateway שונים ולכל הפחות CEF, CLSF ו-syslog. נדרש פירוט לגבי תמיכה בפורמטים נוספים.

~~4.4.5.1.4.~~4.4.5.1.14. נדרש פירוט לגבי היכולת שילוב עם כל Proxy ארגוני אחר ללא הצורך ביצירת Hop נוסף במצב Proxy.

~~4.4.5.1.5.~~4.4.5.1.15. נדרש כי שילוב השירות/המערכת עם מכשירים ניידים לא יפריע לאפליקציות המותקנות על המכשירים ואשר מכילות Hardcoded URI.

~~4.4.5.1.6.~~4.4.5.1.16. נדרש כי השירות/המערכת תכיל ממשק משתמש פשוט תוך הרשאות גישה מבוססת פרופילי משתמשים.

~~4.4.5.1.7.~~4.4.5.1.17. נדרשת זמינות מערכת תוך תמיכה ב Recovery Time Objective=0.

~~4.4.5.1.8.~~4.4.5.1.18. נדרשת תמיכה ביכולת גידול הכוללת את משתמשי המערכת, ההתקנים. נדרש פירוט לגבי יכולת המערכת לספק גידול, דרישות חומרה, תוכנה ונפחי אחסון.

~~4.4.5.1.9.~~4.4.5.1.19. נדרש פירוט לגבי ביצועי המערכת ונתוני Latency בהתאם לאופן הטמעת המערכת.

~~4.4.5.1.10.~~4.4.5.1.20. נדרש פירוט לגבי תכונות פתרון ה CASB ליישום מדיניות מערכות מבוססות ענן.

~~4.4.5.1.11.~~4.4.5.1.21. נדרש פירוט על יכולת התממשקות לשירותי ענן באמצעות ממשקי API.

~~4.4.5.1.12.~~4.4.5.1.22. נדרשת תמיכה בקישור לאפליקציות ענן חדשות. נדרש פירוט לגבי SLA במקרה של קישור אפליקציית ענן חדשה.

~~4.4.5.1.13.~~4.4.5.1.23. נדרשת יכולת מובנית ויכולת הגדרה ידנית בנוגע ליצירת רמות שונות לגישה לנתונים (RBAC) והגדרות אפליקטיביות, בהתאם לקביעת מנהל המערכת.

~~4.4.5.1.14.~~4.4.5.1.24. נדרשת יכולת יצירת חוקה על בסיס AD Attributes

~~4.4.5.1.15.~~4.4.5.1.25. נדרשת יכולת אכיפת בקרת גישה על אפליקציות באופן מותאם אישית ועל סמך פרמטרים כמו :

~~4.4.5.1.15.1.~~4.4.5.1.25.1. Device.

~~4.4.5.1.15.2.~~4.4.5.1.25.2. Location.

~~4.4.5.1.15.3.~~4.4.5.1.25.3. User.

~~4.4.5.1.15.4.~~4.4.5.1.25.4. Activity.

~~4.4.5.1.15.5.~~4.4.5.1.25.5. במידה והפתרון תומך באכיפה על סמך פרמטרים נוספים, יש לפרט זאת.

~~4.4.5.1.16.~~4.4.5.1.26. נדרשת אינטגרציה עם מערכות כדוגמת Microsoft Graph APIs לניטור פעילויות המשתמשים ואכיפת מדיניות.

4.4.5.2. זיהוי והצגת נתוני פלטפורמות, אפליקציות ותשתיות ענן

4.4.5.2.1. נדרשת תמיכה בפתרון CASB אינטגרטיבי המנוהל באמצעות מערכת ניהול מרכזית אחודה.

~~4.4.5.2.2. נדרשת תמיכה זיהוי והצגת "Shadow IT".~~

~~4.4.5.2.3.~~4.4.5.2.2. נדרש פירוט על אופן התמיכה בזיהוי והצגת שירותי IaaS ו-PaaS בשימוש, וכן על המידע המוצג.

~~4.4.5.2.4.~~4.4.5.2.3. נדרשת תמיכה בזיהוי והצגת משתמשי יישומי ענן, על בסיס שם או User ID.

4.4.5.2.5 4.4.5.2.4. נדרשת תמיכה בזיהוי והצגת מכשיר ודפדפן ספציפיים עבור משתמשי יישומי ענן.

4.4.5.2.6 4.4.5.2.5. נדרשת תמיכה בזיהוי והצגת מידע אודות מיקום גיאוגרפי ו-IP, ממנו מתבצעת גישה.

4.4.5.2.7 4.4.5.2.6. נדרשת תמיכה בזיהוי נתונים (קבצים, שדות) מאוחסנים או בשימוש עם שירותי הענן אשר זוהו ולהציגם כפריטים בעלי סיכון נתונים משמעותי.

4.4.5.2.8 4.4.5.2.7. נדרשת תמיכה ביצירת מדיניות DLP, נדרש פירוט לגבי יכולת DLP גם במהלך העלאת קבצים מוגני סיסמה, נעולים/מוצפנים לענן, על מנת לאפשר ל-CASB לבדוק ולהגן על נתונים קריטיים בתאים, עמודות, הערות על גבי מסמכים ומטא נתונים. נדרש פירוט לגבי תכונות נוספות כולל תמיכה במילונים ומנגנוני אימות נתונים הכוללים מידע אישי מזהה (PII), מידע בריאותי מוגן (PHI), מספרי תעודת זהות, כרטיסי אשראי, מספרי לקוחות וכו'.

4.4.5.2.9 4.4.5.2.8. נדרשת תמיכה בניטור נתונים, תוך שימוש בממשקי ה-API אשר מסופקים על ידי אפליקציית הענן ולאפשר יצירת מדיניות הצפנה או התראה על הפרת מדיניות שימוש בסוגי אפליקציות שונות. נדרש פירוט לגבי יכולות יצירת ממשקים ואינטגרציה עם מערכות ענן.

4.4.5.2.10 4.4.5.2.9. נדרש פירוט לגבי תמיכה בפתרונות גמישים לניהול מפתחות הצפנה, כולל מפתחות המנוהלים בפתרון מקומי או רכיב HSM מבוסס ענן.

4.4.5.2.11 4.4.5.2.10. נדרשת תמיכה בניטור נתונים, באמצעות חיבור Proxy בין המשתמש לאפליקציית הענן ויצירת מדיניות חסימה, הצפנה או התראה על הפרת מדיניות שימוש בסוגי אפליקציות שונות.

4.4.5.2.12 4.4.5.2.11. נדרשת תמיכה בבדיקת תעבורה הנשלחת באמצעות HTTPS והפעלת מדיניות בעת הטמעת Proxy In-Line.

4.4.5.2.13 4.4.5.2.12. נדרשת תמיכה-בשילוב תגיות זיהוי מיישומים מקומיים או יישומי צד שלישי ושילובם במדיניות. נדרש פירוט לגבי היכולת לשלב מידע ממערכות ניהול זכויות מידע DRM/IRM על מנת למנוע העתקה, הדפסה או הפצה של מסמכים רגישים.

4.4.5.2.14 4.4.5.2.13. נדרש פירוט לגבי תמיכה במודעות מבוססת מיקום לנושאי אחסון ושילובו במדיניות על המערכת לתמוך ביכולות ציות ועמידה בדרישות אזורי שיפוט שונים.

4.4.5.2.14. נדרשת אינטגרציה עם מערכות EMM. נדרש פירוט לגבי יכולת יצירת מדיניות מבוססת שילוב מערך EMM ארגוני ושילוב התקני BYOD בלתי מנוהלים.

4.4.5.2.15. נדרשת תמיכה בסיווג ותיעדוף שירותי ענן ויצירת מדיניות בקרת גישה על בסיס רמת האמון אשר יקבע הארגון. לדוגמה, שירותים "מהימנים" אשר מותרים לגישה לכלל

משתמשי הארגון; שירותים "לא מהימנים" החסומים בכל עת; ושירותים "לא מהימנים לחלוטין" שיש לפקח ולבקר בקפידה בזמן שמתקבלת החלטה על אפליקציית ענן מסוימת.

4.4.5.3. בקרת גישה

~~4.4.5.3.1. נדרשת תמיכה בסיווג ותעדוף שירותי ענן ויצירת מדיניות בקרת גישה על בסיס רמת האמון אשר יקבע הארגון. לדוגמה, שירותים "מהימנים" אשר מותרים לגישה לכלל משתמשי הארגון; שירותים "לא מהימנים" החסומים בכל עת; ושירותים "לא מהימנים לחלוטין" שיש לפקח ולבקר בקפידה בזמן שמתקבלת החלטה על אפליקציית ענן מסוימת.~~

~~4.4.5.3.2.~~4.4.5.3.1 נדרשת תמיכה באינטגרציה עם תשתית אבטחה ארגונית לניהול מערך זיהוי המשתמשים - בין אם פנימי או מבוסס ענן. כולל יכולת Single Sign On.

~~4.4.5.3.3.~~4.4.5.3.2 נדרשת תמיכה בטכנולוגיות ופרוטוקולי אימות ומתן הרשאות. נדרש פירוט לגבי תמיכה בפרוטוקולים כדוגמת SAML, ADFS, OAuth ו-SCIM.

~~4.4.5.3.4.~~4.4.5.3.3 נדרשת יכולת הזדהות חזקה מבוססת מדיניות, תוך שילוב פתרונות ארגוניים, מקומיים או מבוססי ענן. נדרש פירוט לגבי יכול משתמש מסוים להפעיל מדיניות המבוססת אירועים, אשר יובילו לדרישה מהמשתמש לספק שכבת זיהוי נוספת.

~~4.4.5.3.5.~~4.4.5.3.4 נדרשת תמיכה בזיהוי נתונים ולכל הפחות משתמש, מכשיר, מיקום, שירות, רשת, שעה וסוג הנתונים לצרכי שילוב בחוקה ובמדיניות.

~~4.4.5.3.6.~~4.4.5.3.5 נדרשת תמיכה בבקרת גישה על סמך פעולות המשתמש על בסיס מהימנות הגישה. כלומר במידה ולדוגמה החליט הארגון כי-Google Drive איננו "מהימן", ואילו Microsoft OneDrive מוגדר כ "מהימן"– יכול המשתמש להוריד מסמך אשר שותף עמו ב-Google Drive אך לא יכול להעלות ליעד זה מסמכים.

~~4.4.5.3.7.~~4.4.5.3.6 נדרשת יכולת הגדרה ויישום מדיניות על בסיס הרשאות משתמש לשימוש בשירותי ענן ולדוגמה אישור שימוש ב Dropbox ארגוני, ללא יכולת שימוש בשירות אישי של המערכת.

~~4.4.5.3.8.~~4.4.5.3.7 נדרשת יכולת הגדרת דרישות בקרת גישה ספציפיות למדינה, כגון מתן גישה לפלטפורמת CRM בענן מארה"ב, קנדה והאיחוד האירופי, אך חסימת גישה ממדינות אחרות.

4.4.5.4. ניהול סיכוני Cloud Service Providers

4.4.5.4.1. נדרש כי ספק ה-CASB יבצע סקירות שנתיות כדוגמת SOC II type 2. מידע

לגבי הסקר ותדירותו נדרש להיות זמין בממשק המשתמש.

4.4.5.4.2. נדרש פירוט מיצרן המערכת לגבי עמידה בתקנים נוספים ופעילויות הערכת סיכונים המבוצעות על ידו באופן שוטף.

4.4.5.5. זיהוי איומים

4.4.5.5.1. נדרשת תמיכה ביומן פעילויות מלא (Audit Trail). נדרש פירוט לגבי נתונים הנשמרים ביומן הפעילות ומשך זמן אחסון הנתונים.

4.4.5.5.2. נדרש פירוט על יכולות המערכת לבצע Behavior Analysis כולל ניטור פעילות המשתמש וזיהוי חריגות מחוקה ומדיניות מוגדרת.

4.4.5.5.3. נדרשת תמיכה במנגנוני זיהוי חשבונות החשודים כי נפגעו וביצירת פעולות אוטומטיות לתיקון החשבונות, כגון יצירת התראה וחסימת גישה לחשבון הספציפי.

4.4.5.5.4. נדרשת תמיכה בהעברת חריגים ממדיניות לקבוצת Analysts מוגדרת מראש לטובת פעילות חקירה. נדרש פירוט לגבי יכולת לספק נתונים לצוותי התגובה לאירועים (Incident Response Team) ולצוותים פורנזיים לאחר התרחשות פעילות חשודה.

4.4.5.5.5. נדרש פירוט לגבי יכולת אינטגרציה לקונסולות ניהול של ספקי IaaS על מנת למנוע נזק אשר עלול להשפיע על יישומים הפועלים בפלטפורמות אלה במידה ונפגע חשבון משתמש פריבילגי (Administrator).

4.4.5.5.6. נדרשת יכולת הפקת התראות בזיהוי אנומאליות בשירותי הענן.

4.4.5.5.7. נדרשת תמיכה בניטור נתונים המאוחסנים באפליקציות ענן וזיהוי תוכנות זדוניות בקבצים. על יכולת זו להתאפשר בזמן אמת וגם בסריקת Ad-Hoc תוך אינטגרציות מבוססות API.

~~4.4.5.6.~~4.4.6. **דוחות**

4.4.6.1. נדרשת תמיכה בהצגת כלל אירועי המערכת, כולל פעולות ניהול ואדמיניסטרציה וכן האיומים בתצוגה עדכנית והיסטורית על גבי Dashboard אחוד המאפשר יכולת גישה ותחקור של הראיות הפורנזיות.

4.4.6.2. נדרש פירוט ליכולת יצירת דוחות הכוללים פרמטרים כדוגמת מכסות נפחים עבור הורדה/העלאה, מגבלת מכסת גלישה באינטרנט עבור משתמשים/קבוצות.

~~4.4.5.6.1.~~4.4.6.3. נדרש פירוט לגבי יכולות תצוגה ואפיון של Dashboard המערכת.

~~4.4.5.6.2.~~4.4.6.4. נדרשת תמיכה ב-Audit Trail מלא כולל יכולת איסוף נתונים על פעילות משתמשי הקצה ופעילות מנהלי המערכת ובאינטגרציה למערכות SIEM. נדרש פירוט על מערכות SIEM נתמכות, ובכלל זה לציין את היקף התמיכה ב-Google Chronicle. ~~מובילות (בהתאם לריבוע הקסם של גרטנר).~~

4.4.5.6.3.4.4.6.5 נדרשת תמיכה ביצירת דוחות מותאמים תקינה ורגולציה. נדרש פירוט לגבי סוגי דוחות לדוגמה; ISO,SOX, PCI, FISMA ו-GLBA.

4.4.5.6.4.4.4.6.6 נדרש פירוט לגבי אופן הפקת הדוחות ותקנים נוספים נתמכים.

4.4.5.6.5.4.4.6.7 נדרשת תמיכה בהפקת דוחות קיימים ומוגדרים מראש וכמו כן יצירת דוחות מותאמים אישית.

4.4.5.6.6.4.4.6.8 נדרש פירוט בנוגע למערך הדוחות הקיימים במערכת ותהליך הפקת דוחות מותאמים מראש.

4.4.5.6.7.4.4.6.9 נדרשת תמיכה בהפקה וייצוא דוחות. נדרש פירוט על הפורמטים הנתמכים, כדוגמת: PDF, Word, Excel, Html.

4.4.5.6.8.4.4.6.10 נדרש פירוט לגבי תזמון הפקת דוחות וערוצי הפצתם ופורמטים נוספים הנתמכים על ידי המערכת.

4.4.5.6.9.4.4.6.11 נדרשת תמיכה ביכולת שמירת רשומות למשך 12 חודשים, לכל הפחות. נדרשת תמיכה ביכולת גיבוי יומני המערכת והפקת דוחות חודשיים.

4.4.5.7.4.4.7 ניהול משתמשים

4.4.5.7.1.4.4.7.1 נדרש כי הפתרון יתמוך במערך ניהול מרכזי כדוגמת Active Directory לצורך אימות ומתן הרשאות משתמשים. כמו כן נדרש פירוט לגבי אינטגרציה עם פתרונות PIM/PAM.

4.4.5.7.2 נדרשת תמיכה הכוללת שדרוגי גרסאות, עדכוני תיקון, כולל זמינות באתר המזמין במידת הצורך על בסיס דרישות ה-SLA למכרז.

4.4.5.7.3.1.1.1.1 נדרש פירוט ליכולת יצירת דוחות הכוללים פרמטרים כדוגמת מכסות נפחים עבור הורדה/העלאה, מגבלת מכסת גלישה באינטרנט עבור משתמשים/קבוצות.

4.4.5.7.4.4.4.7.2 נדרשת יכולת הקצאת סט מוגדר של מדיניות מדיניות ניהול משתמשים על גבי מספר Tenants.

4.4.5.7.5.4.4.7.3 נדרש לאפשר למנהל המערכת לאכוף את המדיניות באופן סלקטיבי עבור משתמשים מרוחקים (ענן ממשלתי פרטי וציבורי) מאותה מערכת ניהול.

4.4.5.7.6.1.1.1.1 **נדרשת תמיכה בהגנה מפני מתקפות** Zero Day למשתמשים בנדידה.

4.4.5.7.7.1.1.1.1 **נדרשת** תמיכה בהגנה מפני ניצול פגיעויות על גבי דפדפנים (כדוגמת HTML Smuggling). נדרש פירוט לגבי אופן היישום, מנועי סריקה ויכולות נוספות בנושא זה.

4.4.5.7.8.1.1.1.1 **נדרשת יכולת** SSL Inspection למשתמשים מקומיים ולמשתמשים בנדידה.

4.4.5.7.9.1.1.1.1 **נדרש פירוט לגבי יכולת הגדרת אישור או חסימת תעודות בלתי מוכרות** (Untrusted Certificates).

4.4.5.7.10.1.1.1. נדרשת יכולת גישה למסדי נתונים מקוונים ואו מקומיים לקטלוג URL's כוודוניים, מאושרים. נדרש פירוט לגבי יכולות SSL Inspection, חסימה, ניטור הHostname/IP address על בסיס נתוני ערך הסיכון (Risk Score).

4.4.5.7.11.1.1.1. נדרש פירוט לגבי כמות הקטגוריות הנתמכות על ידי מודול הגישה המאובטחת ל Web. נדרש פירוט לגבי כמות הקטגוריות אליה יכולה להיות משויכת כתובת URL. נדרש פירוט לגבי יכולות קביעת החוקה על בסיס קטגוריות אלה.

4.4.5.7.12.1.1.1. נדרשת תמיכה ביצירת קטגוריה מותאמת אישית וצירוף כתובות URL באופן ידני לקטגוריה.

4.4.5.7.13.1.1.1. נדרשת יכולת הגדרת מדיניות על בסיס קטגוריות מוגדרות מראש ומותאמות אישית כגון שיתוף קבצים, הימורים ועוד.

4.4.5.7.14.1.1.1. נדרשת תמיכה בפרוטוקולים הבאים:

4.4.5.7.14.1.1.1.1. TLS1.3.

4.4.5.7.14.2.1.1.1. HTTP/3.

4.4.5.7.14.3.1.1.1. HTTPS.

4.4.5.7.14.4.1.1.1. DoH.

4.4.5.7.14.5.1.1.1. IPv6.

4.4.5.7.15.1.1.1. נדרשת תמיכה בהצפנה מלאה בין הClient לשרתי ה Proxy. נדרש פירוט לגבי אופן התמיכה בפרוטוקול ופרוטוקול נתמכים נוספים.

4.4.5.7.16.1.1.1. נדרשת תמיכה בזיהוי פגיעויות (Malware Detection) על בסיס חתימות (Signatures). נדרש פירוט לגבי תמיכה בזיהוי על גבי מכשיר המשתמש.

4.4.5.7.17.1.1.1. נדרש פירוט לגבי מנועי Sandbox מוטמעים.

4.4.5.7.18.1.1.1. נדרשת תמיכה בזיהוי פעילות זדונית או פעילות על טכנולוגית (Shadow IT). נדרש פירוט לגבי אופן ויכולות הזיהוי.

4.4.5.7.19.1.1.1. נדרשת תמיכה בחשיפת מידע (Metadata) באשר לשירות הענן אליו קיימת גישה למשתמשי הארגון:

4.4.5.7.19.1.1.1.1. פונקציונליות (כגון: מדיה חברתית, שיתוף קבצים).

4.4.5.7.19.2.1.1.1. האזור ממנו מסופק שירות הענן.

4.4.5.7.19.3.1.1.1. נקודות תורפה ידועות של שירות הענן.

4.4.5.7.20.1.1.1. חישוב הסיכון הכללי עבור שירות הענן, נדרש פירוט לגבי יכולת המשתמש לצפות בפרמטרים אשר הובילו לחישוב הסיכון).

4.4.5.7.21.1.1.1. נדרש פירוט לגבי מדיניות הצפנה לנתונים המאוכסנים בשירות הענן.

~~4.4.5.7.22.1.1.1 נדרש פירוט לגבי פרוטוקולי הצפנה המשמשים להעברת נתונים בשירות הענן.~~

~~4.4.5.7.23.1.1.1 נדרשת תמיכה בהערכת ציות שירותי הענן אל מול התקינות/רגולציות הבאות:~~

~~4.4.5.7.23.1.1.1.1 GDPR.~~

~~4.4.5.7.23.2.1.1.1 PCI.~~

~~4.4.5.7.23.3.1.1.1 ISO.~~

~~4.4.5.7.23.4.1.1.1 HIPAA.~~

~~4.4.5.7.23.5.1.1.1 נדרש פירוט לגבי תמיכה בתקינה או רגולציה נוספת, כדוגמת CSA.~~

~~4.4.5.7.24.1.1.1 נדרש פירוט לגבי תמיכה, בכל מקרה של פרצת אבטחה אצל ספק שירותי ענן, בדיווח אשר כולל פרטי הפריצה ומידע על שימוש העובדים בשירות הענן הנפרץ.~~

~~4.4.5.7.25.1.1.1 נדרש פירוט לגבי יכולות מניעת דלף מידע. נדרש פירוט לגבי מאפיינים לפונקציונליות זאת תוך שימוש ובהיעדר שימוש בסוכן.~~

~~4.4.5.7.26.1.1.1 נדרש פירוט לגבי תמיכה להגדרת התראה ב False Positive או ב False Negative לצורך טיוב מנוע הסיכונים.~~

~~4.4.5.7.27 נדרשת תמיכה בהגדרת Watch list לניטור משתמשים נבחרים המזהים התנהגות חשודה.~~

~~4.4.5.7.28 נדרשת תמיכה ביכולת עריכת דפים חסומים.~~

~~4.4.6 נדרש פירוט בנוגע לתמיכה ביכולת אכיפת מדיניות גם כאשר יחידת הקצה איננה מקוונת.~~

~~4.4.6.1.~~4.4.8 **דיווח והתראות**

~~4.4.6.1.1.~~4.4.8.1 נדרשת יכולת יצירת וסינון דוחות מערכת (דוחות מובנים ודוחות מותאמים אישית). נדרש פירוט לגבי סוגי הדוחות הכלולים במערכת וממשק יצירת הדוחות המותאמים.

~~4.4.6.1.2.~~4.4.8.2 נדרש פירוט על יכולת שליחת התראות למנהלי המערכות ולגורמים אשר יוגדרו מראש בזמן אמת ובאופן מתוזמן. ~~יש~~ נדרש פירוט ~~לפרט~~ לגבי יכולות המערכת לשליחת התראות (אופן שליחה, תוכן, תזמון וכו') והאם יכולת זו מובנית במערכת או שהמערכת תומכת באינטגרציה לכלים לניהול ההתראות.

~~4.4.6.1.3.~~4.4.9 **ניהול שינויים ו-Best Practice**

~~4.4.6.1.3.1.~~4.4.9.1 נדרש פירוט על ה-Best Practice של היצרן לגבי אופן הטמעת המערכת.

~~4.4.6.1.3.2.~~4.4.9.2 נדרש פירוט על מתודולוגיית העדכונים של המערכת ואופן התקנתם באופן שיבטיח כי כל שינוי ייבחן ויאושר טרם הטמעתו בסביבת הייצור.

~~4.4.6.2.~~4.4.10 **מפת דרכים**

~~4.4.6.3.~~4.4.10.1 נדרש פירוט לגבי מפת הדרכים של היצרן בתחום התיחור, תוך התמקדות בתכונות מרכזיות (Main Features) וכן לוחות זמנים לשנה הקרובה.

~~4.4.6.4.~~4.4.11 **תשתית המערכת**

~~4.4.6.4.1.~~4.4.11.1 השירות יופעל על גבי פלטפורמת הענן הציבורי של אחד מהזוכים – Amazon Web Services ו-Google (להלן: "**ספקי הענן**") במכרז 01-2020 לאספקת שירותי ענן על גבי פלטפורמה ציבורית עבור משרדי הממשלה ויחידות הסמך (להלן: "**מכרז נימבוס**"), וזאת בהתאם לכללים המפורטים להלן:

~~4.4.6.4.2.~~4.4.11.1.1 השירות נדרש לפעול מאזור ענן ציבורי המוקם על ידי אחד מספקי הענן בשטח הטריטוריאלי של מדינת ישראל ואושר על ידי עורך המכרז (להלן: "**האזור הישראלי**"), וזאת לא יאוחר מ-12 חודשים ממועד ההכרזה על מועמד לזכייה, או תוך 6 חודשים מהמועד בו ספק הענן אישר כי האזור הישראלי ערוך להפעלת השירות בהתאם לדרישות מהספק בהתאם לסעיף 4.4.11.1.2 ~~4.4.14.1.3~~4.4.14.1.2 ~~4.4.5.10.3~~להלן, המאוחר מבינהם.

~~4.4.6.4.3.~~4.4.11.1.2 אם טרם הוקם האזור הישראלי של ספק הענן אשר המערכת מוצעת על בסיס פלטפורמת הענן שלו, תסופק המערכת, באופן זמני ועד הקמת האזור הישראלי, על בסיס אזור הענן הציבורי הגדול ביותר שמופעל על ידי ספק הענן בו מופעלת המערכת המוצעת בתחומי האיחוד האירופי (להלן: "אזור חו"ל"). במקרה זה, הספק יעביר את המערכת, לרבות נתוני המשתמשים, לאזור הישראלי תוך 6 חודשים מהיום בו ספק הענן אישר כי האזור הישראלי ערוך להפעלת המערכת בהתאם לדרישות מהספק. העברת נתוני המשתמשים תבוצע בתיאום עם המזמינים וללא עלות נוספת.

~~4.4.6.4.4.~~4.4.11.1.3 המערכת תידרש לעמוד בכל התקנים הנדרשים וב-SLA, לכל המאוחר, תוך 12 חודשים נוספים מהיום שבו המערכת החלה להיות מסופקת באזור הישראלי, המוגדר במכרז זה.

~~4.4.6.4.5.~~4.4.11.1.4 השירות יופעל באזור הישראלי בהתאם לתצורה המקובלת על ידי הספק להצעת השירות באזורים אחרים בחו"ל בהם השירות פרוס, ובכל מקרה יהיה פרוס ויוצע למזמינים ביותר ממתחם (Availability Zone) אחד באזור הישראלי, באופן שיבטיח את שרידות השירות והמשך אספקתו גם במקרה של נפילת מתחם אחד. למען הסר ספק, האיזור הישראלי יפעל באופן עצמאי לחלוטין ויוכל לפעול גם ללא תקשורת לאזורים אחרים של היצרן.

~~4.4.6.4.6.~~4.4.11.2 יש לפרט את תצורת המערכת לרבות התייחסות לנושאים הבאים:

~~4.4.6.4.6.1.~~4.4.11.2.1 תשתיות הענן הציבורי עליהם הפתרון מבוסס, מבין פלטפורמות ספקי הענן.

~~4.4.6.4.6.2.~~4.4.11.2.2 האם החשבון עליו פועלת המערכת הינו ייעודי למערכת המוצעת או שהינו משותף לכלל המזמינים.

~~4.4.6.5.~~4.4.11.3 תצורת עבודת המערכת המוצעת

~~4.4.6.5.1.~~4.4.11.3.1 יש לפרט את תצורת פעולת המערכת המוצעת תוך התייחסות לנקודות הבאות:

~~4.4.6.5.1.1.~~4.4.11.3.1.1 מיקום שמירת מידע מוגן – ב-"רשת" (כגון VPC) של המזמין,

אצל הספק, אצל היצרן או בכל מקום אחר. אם המידע אינו נשמר אצל המזמין יש לפרט את מיקום שמירתו, לרבות המדינה והגוף בהם נשמר הידע.

4.4.11.3.1.2~~4.4.6.5.1.2.~~ 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 מקום שמירת נתוני התוכן, לרבות המדינה והגוף אצלם נשמרים הנתונים.

4.4.11.3.1.3~~4.4.6.5.2.~~ אם שמירת החומר והעיבוד הינה אצל המזמין, יש לפרט את יכולת הגישה או השליטה של הספק או היצרן על המידע או המערכת אם ישנה.

4.4.11.3.2~~4.4.6.5.3.~~ יש לפרט את תצורת קישור המערכת לרשת המזמין תוך התייחסות לנקודות הבאות:

4.4.11.3.2.1~~4.4.6.5.3.1.~~ 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.

4.4.11.3.2.2~~4.4.6.5.3.2.~~ 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.

4.4.11.4~~4.4.6.6.~~ אבטחת ההון האנושי

4.4.11.4.1~~4.4.6.6.1.~~ יש לפרט את תהליכי הבקרה, האימות והסינון המתבצעים לעובדי היצרן וספקי המשנה שלו, תוך התייחסות להבדלים בתהליכים בהתאם לסוגי העובדים ורמות הסיכון הגלומות בתפקידם.

4.4.11.4.2~~4.4.6.6.2.~~ יש לפרט את תהליכי ההכשרה והריענון לנהלי האבטחה, הביטחון והסייבר לעובדי היצרן וספקי המשנה שלו.

4.4.11.4.3~~4.4.6.6.3.~~ יש לפרט את תהליכי ההכשרה וההסמכה המקצועית של אנשי המקצוע של היצרן ושל ספקי המשנה שלו.

4.4.11.4.4~~4.4.6.6.4.~~ יש לפרט את מנגנוני הפיקוח על קיום הנהלים ואופן הטיפול בהפרות נהלי אבטחה או נהלים קריטיים אחרים.

4.4.11.4.5. 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.

~~.4.4.6.6.5~~

~~4.4.6.7.~~4.4.11.5. אבטחת שרשרת האספקה

~~4.4.6.7.1.~~4.4.11.5.1. 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, אם יש.

~~4.4.6.7.2.~~4.4.11.5.2. יש ~~לתאר~~ לפרט את אמצעי האבטחה על שרשרת האספקה לרבות הנושאים הבאים:

~~4.4.6.7.3.~~4.4.11.5.2.1. תהליכי הבקרה על הכנסת תוכנה ממקור חיצוני והעדכונים לה, לרבות איתור חולשות, backdoors או הטמנות עם יכולות פוגעניות.

~~4.4.6.7.4.~~4.4.11.5.2.2. תהליכי הבקרה על הכנסת תוכנה ממקור פנימי והעדכונים לה, לרבות איתור חולשות, backdoors או הטמנות עם יכולות פוגעניות.

~~4.4.6.7.5.~~4.4.11.5.2.3. יש ~~לתאר~~ לפרט כל תהליך או בקרה רלוונטיים נוספים.

~~4.4.6.7.6.~~4.4.11.5.3. יש ~~לתאר~~ לפרט את תהליך הפיקוח והבקרה על ספקי המשנה, לרבות התקנים לפיהם הבקרה מתבצעת.

~~4.4.6.8.~~4.4.11.6. המידע הנאגר אצל היצרן

~~4.4.6.8.1.~~4.4.11.6.1. יש לפרט את המידע הנאגר אצל היצרן במהלך מתן השירותים, כגון נתוני עיבוד (כהגדרת המונח להלן) או נתוני גישה (כהגדרת המונח להלן).

~~4.4.6.8.2.~~4.4.11.6.2. יש לפרט את מדיניות מחיקת המידע (Retention policy) וכן את המנגנונים המשמשים אותו למחיקת המידע כאשר הדבר נדרש.

~~4.4.6.8.3.~~4.4.11.6.3. אם נשמרים נתונים אצל הספק או היצרן, יש לפרט את אמצעי ההגנה על המידע ואת הכלים והתהליכים הבאים על מנת למנוע גישה בלתי מורשית למידע.

~~4.4.6.8.4.~~4.4.11.6.4. יש לפרט את תהליך מתן הגישה לנתונים אלו ואת קבוצות המשתמשים הרשאים לצפות במידע ואת תהליכי הבקרה לאיתור שימוש לרעה בהרשאות אלו.

~~4.4.6.9.~~4.4.11.7. אבטחת תצורה וניהול שינויים

~~4.4.6.9.1.~~4.4.11.7.1. ~~נדרש~~ כיעל היצרן ~~פועל~~ לפעול על פי מדיניות מסודרת לניהול תצורה ושינויים של כלל המערכות השותפות במתן השירותים, בהתאם לתקנים המקובלים והנדרשים.

~~4.4.6.9.2.~~4.4.11.7.2. יש לפרט את התקן על פיו מבוצעים תהליכים אלו, אם ישנו, תוך תיאור עקרוני של מערכות בקרת התצורה ותהליך בקרה, אישור ותיעוד השינויים.

~~4.4.6.9.3.~~4.4.11.7.3. יש לפרט בקרות למניעת Downgrade לא מאושר של מנגנוני הצפנה, מנגנוני ניהול מפתחות, מערכות הגנה או שירותי הגנה ככל וישנם.

~~4.4.6.9.4.~~4.4.11.7.4. יש לפרט את אופן ההגנה והבקרה בתהליכי הפיתוח, כגון תהליך פיתוח

מאובטח (SDLC) ותקנים רלוונטיים ככל שהיצרן עומד בהם.

~~4.4.6.10.~~4.4.11.8 הגבלת גישת תמיכה

~~4.4.6.10.1.~~4.4.11.8.1 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'.

~~4.4.6.10.2.~~4.4.11.8.2 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.

~~4.4.6.11.~~4.4.11.9 ניהול סיכונים

~~4.4.6.11.1.~~4.4.11.9.1 אם קיים אצל היצרן מנהל אבטחת מידע האחראי על אבטחת המידע בשירותים המוצעים, יש לפרט את תיאור תפקידו והאם הינו חבר הנהלת היצרן.

~~4.4.6.11.2.~~4.4.11.9.2 יש לפרט את תהליכי ניהול הסיכונים אצל היצרן.

~~4.4.6.11.3.~~4.4.11.9.3 יש לפרט את הגורמים המבצעים תהליכים אלו, את דרגי הפיקוח, דרגי האסקלציה לטיפול בסוגיות ואופן הטיפול בממצאים שלא טופלו.

~~4.4.6.11.4.~~4.4.11.9.4 יש לפרט את הכלים, האמצעים ואופן מימושם על מנת לאפשר ניהול הסיכון באופן דינאמי ובהתאם לשינויים במתאר האיומים ובשירותים המסופקים.

~~4.4.6.12.~~4.4.11.10 הזדהות עבור השירות המוצע

~~4.4.6.12.1.~~4.4.11.10.1 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).

~~4.4.6.12.2.~~4.4.11.10.2 יש לפרט את יכולת ההתממשקות עם כלי IdP/IAM למערכות ניהול משתמשים ולמערכות צד ג' לניהול זהויות.

~~4.4.6.12.3.~~4.4.11.10.3 יש לפרט את התמיכה במתן גישה באופן פרטני ברמת תפקידים RBAC – Role Based Access Control, וברמת תכונות ABAC – Attribute Based Access Control.

~~4.4.6.12.4.~~4.4.11.10.4 על השירות לתמוך בקבלת פרטי המשתמשים ממערכת הזדהות מרכזית בפרוטוקולים סטנדרטיים.

~~4.4.6.13.~~4.4.11.11 שרידות והמשכיות עסקית (SLA) של השירות המוצע

~~4.4.6.13.1.~~4.4.11.11.1 ה-SLA של השירות שיינתן מהאזור הישראלי לא ייפול מה-SLA של

השירות בכל אזור אחר. נדרש פירוט לגבי נתוני הזמינות (Uptime) בהם מתחייב לעמוד היצרן.

~~4.4.6.13.2.~~4.4.11.11.2 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'.

~~4.4.6.13.3.~~4.4.11.11.3 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).

~~4.4.6.13.4.~~4.4.11.11.4 יש לפרט את אופן הבקרה של היצרן על איכות השירות הניתן מהאזור הישראלי ואת רמות האסקלציה המוגדרות בנהליו.

~~4.4.6.13.5.~~4.4.11.11.5 ניתן יהיה לגבות או לייצא את נתוני המערכת למצע שבשליטת המזמין באופן שוטף. יש לפרט את פורמט הגיבוי ותאימותו למערכות סטנדרטיות בשוק.

~~4.4.6.14.~~4.4.11.12 הגנת תשתיות השירות

~~4.4.6.14.1.~~4.4.11.12.1 היצרן מפעיל 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. ככל והשירות מופעל על ידי קבלן משנה של היצרן, יש לפרט בנוסף את פרטיו.

~~4.4.6.14.2.~~4.4.11.12.2 יש לפרט שימוש באמצעי הגנה על נקודות קצה (EPP/EDR/XDR) בסביבת היצרן. ככל וקיים כשירות המופעל על ידי קבלן משנה של היצרן (MSSP), יש לפרט בנוסף את פרטיו.

~~4.4.6.14.3.~~4.4.11.12.3 יש לפרט שימוש בכלי אוטומציה לניטור וטיפול באירועים. יש לפרט את מתודולוגיית הפעולה של היצרן (כגון SOAR), הכלים הרלוונטיים ואופן מימושם.

~~4.4.6.14.4.~~4.4.11.12.4 התעבורה הנכנסת והיוצאת לתשתית השירות תנוטר לאיתור תקיפות או פעילות חשודה. יש לפרט את יכולות היצרן בתחום ותהליכי העבודה המיושמים על ידו לצורך כך.

~~4.4.6.14.5.~~4.4.11.12.5 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.

~~4.4.6.14.6.~~4.4.11.12.6 היצרן מבצע שימוש בכלים לניטור רציף של משטח חשיפה של התשתית (Attack Surface Management) – יש לפרט את כל הכלים ותהליכי העבודה בהם נעשה שימוש.

~~4.4.6.14.7.~~4.4.11.12.7 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.

~~4.4.6.14.8.~~4.4.11.12.8 כלל התשתיות, המערכות והשירותים המוצעים מעודכנים בכלל עדכוני האבטחה הרלוונטיים על ידי היצרן. יש לפרט את תהליכי העדכון ותדירות ביצוע העדכונים.

~~4.4.6.14.9.~~4.4.11.12.9 כלל המשתמשים אשר יכולים לגשת למידע של המזמינים או בעלי הרשאות גישה גבוהות (Privileged Access) כגון: Administrators, Operators, DevOps, Support וכו', ינוטרו ויזדהו ברמה גבוהה. יש לפרט את תהליכי העבודה והכלים המיושמים לצורך כך.

~~4.4.6.14.10.~~4.4.11.12.10 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.

~~4.4.6.14.11.~~4.4.11.12.11 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.

~~4.4.6.14.12.~~4.4.11.12.12 יש לפרט את אופן ההגנה על ממשקי API של המערכת, פנימיים וחיצוניים.

~~4.4.6.15.~~4.4.11.13 כלי אבטחה המשמשים להגנת השירותים המוצעים

~~4.4.6.15.1.~~4.4.11.13.1 יש לפרט על כלי ניתוח מתקדמים, אוטומטיים, לרבות משולבי יכולות AI, לאיתור פעילות חשודה בשירותי המשתמשים, ניסיונות לחשיפה או חשיפה של מידע רגיש, וכו'.

~~4.4.6.15.2.~~4.4.11.13.2 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'.

~~4.4.6.16.~~4.4.11.14 הצפנה וניהול מפתחות בשירותים המוצעים

~~4.4.6.16.1.~~4.4.11.14.1 יש לפרט את יכולות ההצפנה של המידע בשכבות השירות השונות.

~~4.4.6.16.2.~~4.4.11.14.2 כלל נתוני המערכת יהיו מוצפנים במנוחה (at rest) ובתנועה (in transit), כברירת מחדל. ככל ולדעת הספק הצפנה זו בלתי ישימה, יש לפרט זאת באופן מלא לרבות בקרות מפצות, אם ישנן.

~~4.4.6.16.3.~~4.4.11.14.3 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.

~~4.4.6.16.4.~~4.4.11.14.4 יש לפרט את אופן ניהול ושמירת המפתחות ביחס לכל אחת משכבות השירות וסוגי השירותים השונים.

~~4.4.6.16.5.~~4.4.11.14.5 יש לפרט לגבי תמיכה בממשק לתשתיות ניהול מפתחות אליהן היצרן מתממשק (כגון KMS).

~~4.4.6.16.6.~~4.4.11.14.6 ככל והיצרן מפעיל תשתית ניהול מפתחות עצמאית, יש לפרט לגבי הפתרון המוצע בדגש על עמידה באופן מלא בתקן FIPS- 140-2 level 2 ומעלה.

~~4.4.6.16.7.~~4.4.11.14.7 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.

~~4.4.6.16.8.~~4.4.11.14.8 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.

~~4.4.6.17.~~4.4.11.15 איסוף לוגים וניטור

~~4.4.6.17.1.~~4.4.11.15.1 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.

~~4.4.6.17.2.~~4.4.11.15.2 יש לפרט את מקורות הלוג האפשריים (כגון: תשתית, תשתית יישומית, יישום, אבטחת מידע וכו').

~~4.4.6.17.3.~~4.4.11.15.3 יש לפרט את עדכניות המידע (הזמן מקרות האירוע עד העברת המידע), היקף המידע, יכולת החקר של המזמין או בא כוחו וכו'.

~~4.4.6.17.4.~~4.4.11.15.4 יש לפרט את פרק הזמן בו נשמרים נתוני העיבוד ונתוני הגישה על ידי היצרן, את מדיניות היצרן בקשר לשמירת נתונים אלו ואופן הגנתם.

~~4.4.6.18.~~4.4.11.16 חקירה

~~4.4.6.18.1.~~4.4.11.16.1 יש לפרט את יכולות היצרן, הכלים ותהליכי העבודה שלו בתחום חקירה ותגובה לאירועי סייבר במערכות היצרן.

~~4.4.6.18.2.~~4.4.11.16.2 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'.

~~4.4.6.19.~~4.4.11.17 בקרה פנימית ועמידה בתקנים

~~4.4.6.19.1.~~4.4.11.17.1 על השירות לעמוד, לכל הפחות, באחד מהתקנים הבאים:

~~4.4.6.19.2.~~4.4.11.17.1.1 תקן ISO27001.

~~4.4.6.19.3.~~4.4.11.17.1.2 תקן SOC 2 AICPA.

~~4.4.6.19.4.~~4.4.11.17.1.3 יש לפרט את התקן בו השירות עומד.

~~4.4.6.19.5.~~4.4.11.17.1.4 יש לפרט תקנים נוספים בהם השירות עומד כגון: ISO27017, ISO27018, CSA STAR level 2 וכו' ככל וקיימים.

~~4.4.6.19.6.~~4.4.11.17.2 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).

~~4.4.6.19.7.~~4.4.11.17.3 יש לפרט את דרגי הפיקוח, דרגי האסקלציה לטיפול באירועים, ואופן הטיפול בממצאים שלא טופלו.

~~4.4.6.20.~~4.4.11.18 הפרדה ומידור לקוחות (Tenants)

~~4.4.6.20.1.~~4.4.11.18.1 יש לפרט את יכולות היצרן, אם ישנן, לבצע בידוד ובידול של Tenant (לקוח) זה או אחר, בהתייחס לנקודות הבאות:

~~4.4.6.20.1.1.~~4.4.11.18.2 אופן ההפרדה והבידול של שירותים משותפים והאמצעים למניעת דלף מידע בין Tenants שונים, גישת משתמשי Tenant מסוים למשאבי Tenant אחר, הפרדת ניהול ובקרה וכו'.

~~4.4.6.20.1.2.~~4.4.11.18.3 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.

~~4.4.6.20.1.3.~~4.4.11.18.4 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.

~~4.4.6.20.2.~~4.4.11.18.5 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

5.1. כל המחירים יכללו אחריות כנדרש בפרק 3 למסמכי המכרז המרכזי וכמפורט לעיל במסמכי התיחור.

5.2. על המציע להזין הצעתו, במחירי המחירון הרשמי, על גבי גיליון האקסל המצורף כנספח ד'1 להודעה על פרסום מסמך התיחור.

5.3. המחירים ייקבעו בתיחור הדינאמי המקוון בהתאם למפורט לעיל.

5.4. **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.

5.5. **הערות**

5.5.1. 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 משתמשים 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.

5.5.2. אם מודל התמחור של המוצר הינו במינוי (Subscription) תחושב העלות לפי המודל הבא:

5.5.2.1. מחיר המינוי לשנה יוכפל ב-5 – בהתאם לאופן 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.

5.5.2.2. לצורך התיחור הדינאמי, ואם יהיה 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.

5.5.2.3. 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~~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' 6 לאספקת מוצרי SSE – Secure Service Edge ושירותים נלווים עבורם המתפרסם במסגרת מכרז מרכזי 05-2022 לרכש ואספקת מוצרים ושירותים בתחום אבטחת המידע והגנה בסייבר עבור משרדי הממשלה ויחידות הסמך ("**התיחור**")

אני, הח"מ_________________, מחברת _____________________________, בעלת הקניין הרוחני של המוצרים והשירותים המוצעים בתיחור ("**היצרן**") על ידי ___________________________ ("**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.

3. המציע מחזיק בהסמכה הגבוהה ביותר של היצרן בתחום התיחור והוא מורשה על ידי היצרן למכור את השירות ולהתחייב לדרישות המכרז והתיחור עבור השירות.
4. היצרן מאשר כי הוא מכיר את תנאי המכרז והתיחור.
5. היצרן מתחייב:

5.1. 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.

5.2. 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.

5.3. 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.

5.4. השירות יופעל באזור הישראלי בהתאם להוראות סעיף ~~4.4.5.10.1~~4.4.11.14 למסמכי התיחור, ובתצורה המקובלת של השירות באזורים אחרים בחו"ל בהם השירות פרוס.

5.5. המענה לנספח ג' לתיחור נעשה באופן התואם את מאפייני השירות ואופן אספקתו על ידי היצרן.

5.6. היצרן יעשה את כל הנדרש ממנו כיצרן על מנת שהמציע יעמוד בתנאי המכרז והתיחור והתחייבויותיו, לכל אורך תקופת ההתקשרות.

5.7. היצרן יעשה את כל הנדרש ממנו על מנת שהמציע יעמוד בתנאי המכרז ובהסכם מכוחו הנדרשים מהיצרן לצורך אספקת השירות, לכל אורך תקופת ההתקשרות.

5.8. 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.

5.9. לעדכן את המציע ועורך המכרז באופן מיידי בדבר פריטים אשר קיימת היתכנות להפסקת ייצורם, שיווקם או התמיכה בהם (END OF SALE, END OF LIFE או END OF SUPPORT) או שכבר הוכרזו ככאלה.

5.10. 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 6 for the supply of Secure Service Edge (SSE) systems 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.

3. 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.
4. The Manufacturer confirms it is familiar with the terms of the Tender and the Specific Invitation.
5. The Manufacturer undertakes a commitment to:
   - 5.1. 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.
   - 5.2. 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.

5.3. 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.

5.4. The service will be operated in the Israeli Region in accordance with the provisions of section 4.4.11.1~~4.4.5.10.1~~ of the Specific Invitation documents, and in the accepted configuration of the service in other overseas regions where the service is deployed.

5.5. 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.

5.6. The Manufacturer will do everything required from him as the Manufacturer, in order for the Bidder to comply with the terms of the Tender, the specific invitation and his commitments, for the duration of the agreement.

5.7. 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.

5.8. 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).

5.9. 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

7.1. אם המציע סבור כי בהצעתו יש חלקים שהם בגדר סוד מסחרי או סוד מקצועי, עליו למלא את הטבלה להלן.

7.2. 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.

7.3. יובהר כי:

7.3.1. מענה המציע על מודל הייחוס (נספח ד׳1), לרבות שמות הפריטים, מק״טים, תיאור הפריטים, מחירים וכמויות, **לא יחשבו** כסוד מסחרי או מקצועי.

7.3.2. מענה המציע על הדרישות הטכניות (**נספח ג׳**) ייחשב כסוד מסחרי או מקצועי ולא תתאפשר זכות עיון בחלק הזה של ההצעה הזוכה בתיחור.

מס״ד	הסעיף/פרק במסמך התיחור	נימוק
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

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

8. נספח ז' – הסבר על מערכת התיחורים הדינאמיים - מערכת מירב

8.1. נספח זה בא להוסיף על האמור במסמכי המכרז המרכזי ובמסמך התיחור, ולא לגרוע מהם.

8.2. נספח זה הינו עבור שלב התיחור הדינאמי המקוון ומהווה חלק בלתי נפרד ממסמכי המכרז המרכזי ומסמכי התיחור.

8.3. בשלב זה – שלב התיחור הדינאמי המקוון – ישתתפו המציעים שנבחרו בהתאם לסעיף 1.4.3~~1.4.3~~ ויתחרו בהתאם לכללים המפורטים בו.

8.4. המסמכים הנדרשים לצורך התיחור הדינאמי פורטו בנספח 2 לחוברת 2 למסמכי המכרז המרכזי.

8.5. **רישום למערכת ההזדהות הלאומית (חד פעמי)**

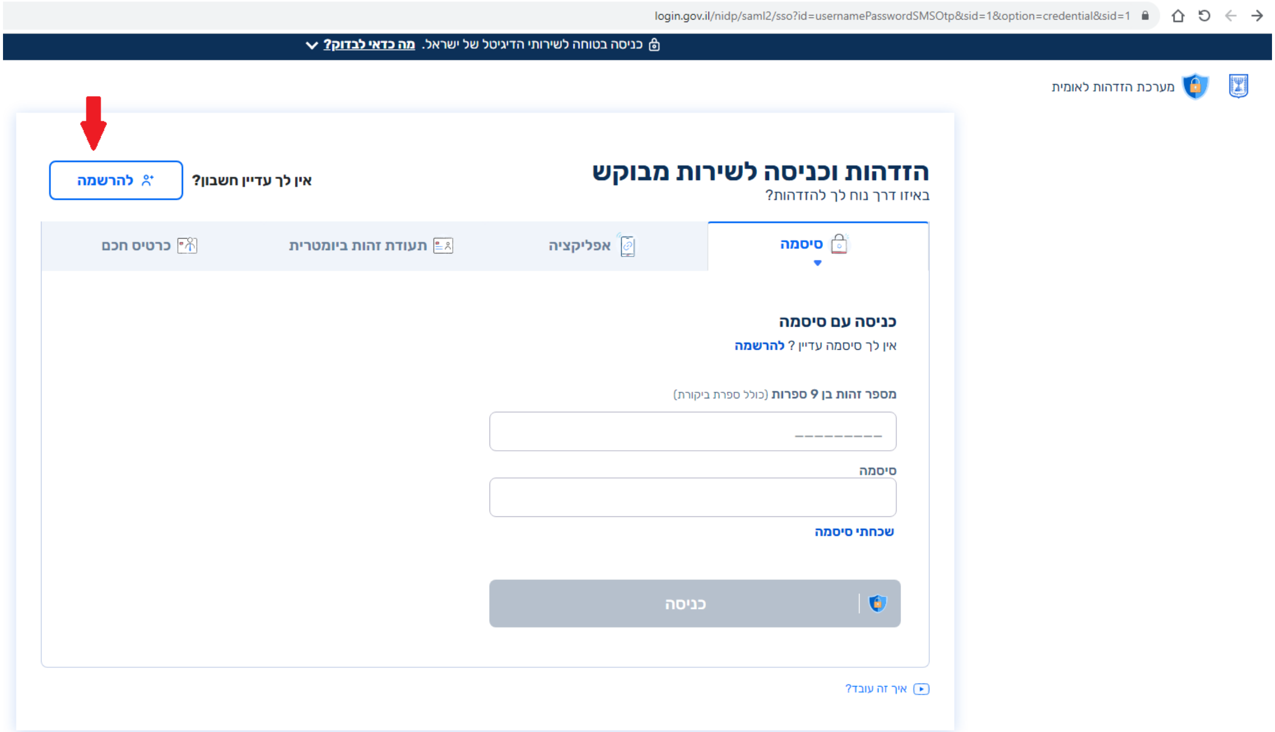
8.5.1. הגשת הצעה תתאפשר, רק למי שיש לו משתמש במערכת ההזדהות הלאומית.

8.5.2. רישום למערכת ההזדהות הלאומית, יבוצע בקישור הבא:

8.5.3. https://account.gov.il/sspr/public/newuser

8.5.4. להלן סרטון הדרכה המסביר את אופן הרישום למערכת הזיהוי הממשלתית: https://www.youtube.com/channel/UCEflHGPEj-M7jtQ0PdzUZkQ

8.5.5. תהליך רישום והזדהות מול מערכות ממשלה שונות כמו גם מערכת מירב, מתבצע באמצעות 'מערכת ההזדהות הלאומית'. רישום למערכת זו נעשה באמצעות מייל פרטי (כדוגמת Gmail) כפי שמופיע בתמונה. לתשומת ליבכם, הרישום ישמש אתכם גם לכניסה לשירותים ממשלתיים שונים לצרכיכם האישיים.



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

8.6. התיחור הדינאמי המקוון

8.6.1.במסגרת התיחור, יתחרו המציעים על מתן מחיר המיטיב ביותר לעורך המכרז עבור הציוד, המוצרים והשירותים הנדרשים במסגרת התיחור.

8.6.2.הצעת המחיר שתוגש על ידי המציע במסגרת התיחור תהיה סופית ותכלול את כל מרכיבי העלות של המוצרים והשירותים המבוקשים הנדרשים לצורך אספקתם וביצועם.

8.6.3.הצעת המחיר במסגרת התיחור תחייב את המציע, אם יזכה, כמפורט במסמכי המכרז המרכזי ובמסמכי תיחור זה.

8.7. מחיר מודל הייחוס

8.7.1. 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.

8.7.2. אם ימצא 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.

8.7.3. 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 הדינאמי המקוון. כמו כן, הוא מחויב ליידע את עורך המכרז בדבר מוצרים אשר, בהתאם להצהרת היצרן, קיימת היתכנות להפסקת ייצורם, שיווקם או התמיכה בהם (End Of Sale, End Of Life או End Of Support) או שכבר הוכרזו ככאלה, והכל כמפורט בחוברת המכרז הראשית.

8.7.4. 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, אם המציע מחויב בגביית מע"מ ("**מחיר מודל הייחוס**"). מחיר מודל הייחוס יהווה את מחיר המקסימום להצעת הפתיחה של כל מציע בתיחור הדינאמי המקוון.

8.7.5. 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.

9. נספח ח' – עיבוד ואבטחת מידע והגנה בסייבר בשירותים

9.1. הגדרות

9.1.1. **אירוע אבטחה** – אירוע (incident) אשר עלול לפגוע בזמינות, מהימנות או סודיות מידע מוגן או השירותים בהם משתמשים המזמינים לרבות תקיפת סייבר.

9.1.2. **הוראה דיגיטלית** – הוראה שניתנה באמצעות כלי התאמה והגדרה (קונפיגורציה) כגון ממשק הניהול של הספק, APIs או כל אמצעי אחר שהועמד לרשות המזמין.

9.1.3. **מידע מוגן** – נתוני עיבוד, נתוני גישה ונתוני תוכן.

9.1.4. **נתוני גישה (Subscription Data)** – כל מידע של משתמשים ומזמינים הנדרשים לצורך ניהול גישה, אספקת השירותים או עבור ביצוע חיובים.

9.1.5. **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).

9.1.6. **נתוני תוכן (Content data)** – בנוסף לאמור בסעיף ~~9.7.1~~9.7.19 להלן, 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.

9.1.7. **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.

9.1.8. **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.

9.1.9. **Service Level Agreement ("SLA")** – הסכם בין ספק שירות למשתמש קצה אשר מגדיר את רמת השירות המצופה מספק השירות וקובע פיצויים בגין חריגה מרמה זו.

9.2. חובה לאבטחת מידע והגנה בסייבר

9.2.1. 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.

9.2.2. 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.

9.2.3. 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.

9.2.4. חובות הספק כלפי המידע המוגן יחולו כל עוד המידע מצוי במערכותיו או במערכות היצרן, גם לאחר תום תקופת ההתקשרות.

9.2.5. הספק יאפשר שמירה ותיעוד מלא של כל גישה ושימוש של המזמין ומשתמשיו לשירותים השונים.

9.2.6. תתאפשר שמירה של התיעוד לתקופה של שנה לפחות כך שיהיה זמין באופן רציף למזמין ולעורך המכרז.

9.3. נתוני תוכן

9.3.1. כלל נתוני התוכן יאוחסנו ויעובדו על גבי פלטפורמות הענן של ספקי הענן.

9.3.2. 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.

9.3.3. 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.

9.4. שימוש במידע

9.4.1. 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:

9.4.1.1. בנתוני תוכן – באישור של המזמין, בהתאם להוראה דיגיטלית, ולצורך אספקה תקינה של השירותים הנרכשים.

9.4.1.2. 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.

9.4.1.3. בנתוני גישה – ברמה המינימאלית הנדרשת לצורך אספקה תקינה של השירותים הנרכשים במסגרת ההסכם, לחיוב בגינם ולמימוש חובותיו של הספק לפי ההסכם.

9.4.2. 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.

9.4.3. 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.

9.4.4. 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.

9.5. מחיקת מידע מוגן

9.5.1. 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. אם השירות 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.

9.5.2. 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.

9.5.3. 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.

9.6. סודיות

9.6.1. 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.

9.6.2. 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.

9.6.3. 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:

9.6.3.1. כי נתונים אלו יוגנו באמצעים הטכנולוגיים המתקדמים ביותר הקיימים בשוק (State of the Art).

9.6.3.2. כי הגישה לנתונים אלו על ידי עובדיו של הספק ייעשה רק על ידי מורשים הנדרשים לצורך כך ורק בהיקף המינימאלי הנדרש.

9.6.4. 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.

9.7. שירות ישראלי

9.7.1. נתוני התוכן ישמרו במלואם בגבולות מדינת ישראל, אלא אם נקבע אחרת במסגרת הסכם זה.

9.7.2. 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.

9.7.3. הוציא הספק מידע מוגן מחוץ לגבולות מדינת ישראל, ימחק את המידע המוגן באופן מידי, ואם הדבר נעשה לצורך מתן שירות בהתאם להוראה דיגיטלית, מיד עם השלמת הפעולה, בהתאם לתנאי ההוראה הדיגיטלית, ובכפוף להוראות הדין.

9.7.4. בכל מקרה ספק לא ישמור מידע מוגן במדינה שאינה מקיימת יחסים דיפלומטיים עם מדינת ישראל.

9.7.5. האמור בסעיף זה יחול על שירות הפועל באזור חו״ל, בהתאמות הנדרשות.

9.8. פרטיות

9.8.1. מבלי לגרוע מחובותיו בנספח ובהסכם, הספק מתחייב לפעול בהתאם להוראות חוק הגנת הפרטיות, התשמ״א-1981 (״**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 (״**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.

9.8.2. הספק יצרף לתנאי השימוש (service agreement) נספח ובו פירוט על העמידה בחובות המוטלות על הספק בהתאם למכרז ותיחור זה ולחוק הגנת הפרטיות ותקנותיו (״**נספח פרטיות**״). לחילופין, יצהיר הספק בכתב על עמידתו בחובות אלו.

9.8.3. עורך המכרז יהיה רשאי לדרוש מהספק לבצע התאמות בנספח הפרטיות, לצורך התאמה להוראות החוק, ההסכם ונספח זה.

9.8.4. 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.

9.8.5. 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.

9.8.6. עבור שירות שאינו ישראלי, הספק לא יוציא מידע פרטי מגבולות אזור המצוי בגבולות האיחוד האירופי ויחולו עליו כללי ה- General Data Protection Regulation (GDPR).

9.8.7. 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.

9.9. איסור פלילי על חשיפת מידע מוגן

9.9.1. 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.

9.9.2. 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).

9.10. דין חל וסמכות שיפוט על מידע מוגן

9.10.1. **מבלי לגרוע מהאמור בסעיף 18 להסכם ההתקשרות**:

9.10.1.1. 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.

9.10.1.2. 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.

9.10.2. 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.

9.11. העברת מידע שלא כדין

9.11.1. על אף האמור בסעיף 9.10.1~~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:

9.11.1.1. 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.

9.11.1.2. אם ישנו צו חיסיון על עצם הבקשה לקבלת המידע, יפעל הספק להסרת הצו, ולמתן אפשרות ליידוע של עורך המכרז על עצם קיומה של הבקשה.

9.11.1.3. יסרב להעברת המידע, ויטען את כל הטענות המשפטיות הרלוונטיות ובכלל זה שהמידע שייך למדינה ריבונית, וכן שהמידע נתון תחת חסינות מדינתית.

9.11.1.4. 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.

9.11.1.5. בהתאם לבקשה של עורך המכרז, יבקש לצרף את ממשלת ישראל כצד להליך הרלוונטי.

9.11.1.6. ידאג לצמצם את היקף חשיפת המידע אך ורק למידע רלוונטי בבקשה.

9.11.1.7. 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.

9.11.2. בנוסף לאמור לעיל, אם תתקבל 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~~9.11.1~~ לעיל, יפעל הספק כמפורט להלן:

9.11.2.1. 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).

9.11.2.2. 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.

9.11.3. מבלי לגרוע מחובות הספק בכל מקום אחר, האמור בסעיף זה יחול על הספק גם במידה והפניה מישות 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.

9.11.4. אם יש לספק אינדיקציה על כך שצפויה להתקבל פניה או צו כאמור בסעיפים 9.10.1~~9.10.1~~-9.11.1~~9.11.1~~ לעיל, הוא יתריע על כך בפני עורך המכרז באופן מידי, אלא אם הוא מנוע על פי דין.

9.12. פעולות נדרשות במקרים של העברת מידע מוגן

9.12.1. 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:

9.12.1.1. 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.

9.12.1.2. 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.

9.12.1.3. 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.

9.12.2. 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.

9.13. <u>חובת הספק לאבטחת מידע וסייבר</u>

9.13.1. 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.

9.13.2. 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.

9.13.3. 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. אם ספק השירות מפעיל חדר מצב להתמודדות עם איומים בסייבר (SOC), הנציג יעביר את פרטי הקשר עם חדר מצב זה לעורך המכרז.

9.13.4. 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.
2. **ניהול שרשרת אספקה וספקים** – הגדרה וקיום מנגנונים שתפקידם לנהל את כל שרשרת האספקה של ספק הענן כדי להבטיח את אמינות התשתיות שבאמצעותן מסופקים השירותים.
3. **ניהול משאבים** – קיום מנגנונים לזיהוי והגנה על נכסים ארגוניים ונכסי מידע ארגוניים, כולל אלה של לקוחות והמזמין.
4. **ניהול אירועי וחשדות לאירועי אבטחה** – קיום אמצעים לניהול, תגובה והעברה של מידע על אירועי אבטחה.
5. **ניהול זהויות והרשאות גישה** – קיום מנגנונים לווידוא כי הגישה למידע מוגן, משאבי עיבוד מידע, מתקנים
6. **רציפות תפקודית והתאוששות** – להבטיח את הרציפות התפקודית של שירותי הענן, כולל התאוששות מאסון

וסביבות וירטואליות הן של משתמשים מורשים בלבד.

תוך הבטחת מהימנות ואמינות המידע בכל עת.

7. **הצפנה וניהול מפתחות** – קיום פעילות מאובטחת של שירותי הספק באמצעות הגדרה ומימוש של מנגנונים קריפטוגרפים נאותים.

8. **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.

9. **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.

10. **שמירה על יכולת הגירה ואינטראופרביליות** – להקצות ללקוח אמצעים שמאפשרים להתממשק לשירותי ענן אחרים או להגר, באופן מאובטח לספקים המספקים שירותים דומים.

11. **שמירה על רציפות תפקודית תפעולית מאובטחת** – וידוא כי מערך הגנת הסייבר של הספק פועל מאובטח ותקין כדי ששירותי הענן יהיו מבצעיים כל העת.

12. **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.

13. **אבטחת תקשורת** – אבטחה של התקשורת הממוחשבת.

14. **ניהול סיכונים** – להקצות את האמצעים הנדרשים לממשל וניהול סיכוני מידע, וכן מנגנונים לאיתור סיכונים להגנת שירותי הענן.

15. **הגנה על מידע אישי** – להקים ולנהל את האמצעים הנדרשים כדי שהמזמינים יממשו את חובותיהם להגן על המידע המצוי בשליטתם.

16. **הליכים נאותים להערכת הגנת הסייבר** – להקים ולנהל תהליכים נאותים לבדיקות הליכי בקרת אבטחה של מערכות ורשתות ליבה של תשתית הענן.

17. **ניהול קונפיגורציה ושינויים** – להקים ולנהל מערכות לניהול שינויים לרשת ולמערכות מידע.

18. **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.

9.14. <u>נהלי הגנת סייבר וניהול סיכונים</u>

9.14.1. 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 ("**מדיניות הסייבר של הספק**").

9.14.2. הספק יבצע הליכי ניהול סיכונים בהתאם לדרישות התקנים בהם הוא עומד ולדרישות החוקים והרגולציות החלות עליו, באופן שוטף.

9.15. <u>תקנים</u>

9.15.1. 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.

9.15.2. 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.

9.15.3. 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.

9.15.4. ככל שתקנים אלו יתעדכנו או שתצא להם גרסה חדשה, יהיה הספק מחויב לעדכנם בהתאם.

9.15.5. הספק יעדכן באופן פומבי את התקנים להם השירות הוסמך.

9.16. <u>עדכונים שוטפים והעברת מידע בנושאי איומי סייבר</u>

9.16.1. הספק ישתף פעולה עם עורך המכרז בנושא ההגנה מפני איומי סייבר, וזאת כחלק ממתן השירותים, בהתאם למפורט להלן:

9.16.1.1. 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.

9.16.1.2. 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.

9.17. התמודדות עם אירועים בזמן אמת ותחקור אירוע

9.17.1. 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.

9.17.2. 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.

9.18. מהימנות עובדים וספקים

9.18.1. הספק יבצע תהליכים מקובלים לבחינת רמת המהימנות של עובדיו, קבלני משנה וספקיו תוך הפעלת תכנית לאיתור ומענה לאיומי אבטחה אשר מקורם בגורם הפנימי.

9.18.2. **מעבדי משנה**

9.18.2.1. 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.

9.18.3. **הנחיות להפעלת מעבד משנה**

9.18.3.1. 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.

9.18.3.2. מעבד המשנה וכל הגורמים המורשים מטעמו לגשת למידע מוגן יהיו חתומים על התחייבות לשמירה על סודיות שתעמוד בחובות הסודיות החלות על הספק.

9.18.3.3. מעבד המשנה עמד בחובה המפורטת בסעיף 9.4.4~~9.4.4~~ לעיל, הקובע כי גישה למידע מוגן יעשה רק לעובדים שהדבר הכרחי עבורם, ורק בהיקף חשיפה בהתאם.

9.18.3.4. הוצאת המידע למעבד משנה אינה אסורה בהתאם לדין (כגון הדין החל לעניין פרטיות וכיוצ״ב).

9.18.3.5. הספק יבצע ביקורות עיתיות לספקי המשנה המספקים שירותים למזמינים.

9.19. אבטחת מידע בשירותים

9.19.1. 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.

9.19.2. 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.

9.19.3. 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.

9.19.4. 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.

9.19.4.1. **<u>ביקורות תקופתיות</u>**

9.19.4.1.1. 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 (״**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.

9.19.4.1.2. 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.

9.19.4.1.3. 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.

9.19.4.1.4. לבקשת עורך המכרז, הספק יעביר לעורך המכרז את תמצית ממצאי הביקורת ואת סטטוס הטיפול בממצאים.

9.19.4.1.5. הספק יישא בעלות הביקורות כאמור.

9.19.4.2. **<u>מבדקי בטחון וחדירות</u>**

9.19.4.2.1. עורך המכרז יהיה רשאי לבצע בקרה על מימוש המדיניות המוגדרת על ידו למזמינים ועל אופן מימושה על תשתיות הספק.

9.19.4.2.2. 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.

9.19.4.2.3. על מנת למזער את הסיכונים הכרוכים במבדקים אלו, מבדקי העמידות יתואמו מראש עם הספק תוך שהספק יימנע מלחסום את הגורמים הבודקים.

9.20. <u>תקיפת סייבר ואירוע אבטחה</u>

9.20.1. בכל מקרה בו אותרה תקיפת סייבר או כל אירוע אבטחה במערכות הספק היכולות להשפיע על המזמינים, ינקוט הספק בפעולות הבאות :

9.20.1.1. 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.

9.20.1.2. הספק ינקוט בכל צעד הנדרש, בהתאם לנסיבות העניין, כדי להפחית את ההשפעות ולמזער את הנזק הנובע כתוצאה מתקיפת הסייבר.

9.20.1.3. הספק יידע את המזמין ועורך המכרז על צעדים שהם יכולים לבצע כדי להפחית את ההשפעות ולמזער את הנזק הנובע כתוצאה מאירוע האבטחה.

9.20.1.4. 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.

9.20.2. הספק ידווח, באופן שוטף, למזמין ולעורך המכרז, על פעולות שהוא ניטר אותן כניסיונות לתקיפת סייבר הממוקדת במערכות המזמינים.

9.20.3. הספק יפיק לקחים מאירועי האבטחה שאירעו ויבחן את הצורך בעדכון המערכות, התהליכים והנהלים.

9.20.4. 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.