## נספח דרישות אבטחת מידע, הגנת סייבר והגנת פרטיות

### 1. כללי

1.1. הספק יהיה האחראי הבלעדי על אבטחת המידע שהועבר או נצבר אצלו במסגרת ההתקשרות. חובת אבטחת המידע וחובת הסודיות מהוות תנאי סף בלתי נפרד בהתקשרות. בנוסף, הספק יהיה אחראי על אבטחת המערכות, התוכנות והחומרה המשמשת אותו לצורך אספקת השירותים או המוצרים למזמין, על תקינותם, אמינותם ושלמותם וזמינותם ועל תפקודם השוטף והתקין. לצורך עמידת הספק בחובות אלו יתפעל הספק ויעדכן את אמצעי האבטחה באופן שוטף, ויוודא כי האמצעים הטכנולוגיים המשמשים לאבטחת המידע הם חדישים ועומדים בסטנדרטים המקובלים בתחום. הספק יקצה משאבים מתאימים במטרה למנוע נזקי סייבר ככלל.

1.2. 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.

1.3. 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, לטפל בהן ולעדכן את מערכותיו מפני חשיפות אבטחתיות בהקדם האפשרי, תוך הפעלת תהליכי מיטיגציה (Mitigation) ככל שלא ניתן לעדכן את המערכות באופן מידי.

1.4. מבלי לגרוע מהאמור, ולצורך עמידה בחובותיו על פי טופס זה מסכים הספק על שיתוף פעולה עם המזמין כמפורט, והכל לצורך ביצוע תקין של התקשרויות עם הנהלת בתי המשפט (להלן הב"ה).

1.5. הספק מתחייב לתקן ליקויים שנמצאו על ידי המזמין בפרק זמן סביר ועל חשבונו, וכן מסכים כי ככול ולא יתקן ליקויים כאמור בפרק זמן סביר, יהווה הדבר הפרה יסודית של ההסכם, ויהווה עילה להפסקת התקשרות בכפוף לשימוע.

1.6. החוזה חל על פי החוק הישראלי ורק בית משפט ישראלי יהיה מוסמך לדון ולהכריע בכל הנוגע לו, פירושו או ביצועו וכל סעד הנובע מאי ביצועו או הפרתו.

1.7. הספק אחראי לשמירה על בטיחות הפעילות באתרי העבודה ובמהלך מתן השירותים, לרבות נקיטת כל האמצעים הנדרשים למניעת סיכונים לעובדים, למשתמשים ולצדדים שלישיים. במסגרת זו, הספק אחראי לפינוי שוטף ומלא של פסולת הנוצרת עקב פעילותו, ובכלל זה פסולת קרטונים, אריזות וחומרים נלווים, בהתאם להוראות הדין, נהלי הבטיחות והנחיות המזמין. הפינוי יבוצע באופן שאינו יוצר מפגע בטיחותי, תברואתי או סביבתי, ועל חשבון הספק בלבד.

## 2. חוקים, תקנות ותקנים

2.1. הספק יהיה אחראי על שמירה, הגנה ושלמות המידע המוגן על מערכותיו, והוא לא ייגש אליו, לא יאפשר לאחר לגשת אליו, לא יעשה בו שום שימוש או שינוי, ולא יתיר כל שימוש או שינוי, בין במעשה ובין במחדל, שאינו מותר בהתאם להוראות הדין הישראלי ובהתאם להוראת ההסכם ונספח זה.

2.2. על הספק לעמוד בתקן אבטחת מידע ארגוני ממשפחת ISO-27001. על הספק לצרף צילום עדכני המעיד על עמידתו בסעיף זה.

2.3. 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.

2.4. הספק מבין כי המידע המוגן כולל מידע על אודות תהליכי העבודה של הנהלת בתי המשפט (להלן "הב"ה")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.

2.5. הספק מתחייב לעמוד בדרישות החוק, התקנות והתקנים המפורטים להלן:

2.5.1. הוראות חוק המחשבים, התשנ"ה 1995.

2.5.2. חוק הגנת הפרטיות ותקנותיו:

2.5.2.1. חוק הגנת הפרטיות, תשמ"א-1981 ותקנותיו השונות לרבות:

2.5.2.1.1. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

2.5.2.1.2. תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001.

2.5.3. דרישות חוק או תקנות בנושא אבטחת מידע, הגנת סייבר והגנת פרטיות הקיימות או יהיו קיימות מטעם גורמי החוק והרגולציה.

2.6. 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.

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

2.8. 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. גכגכה

2.9. 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 (לדוגמה: מידע פרטי, מידע הנתון תחת חיסיון לפי החוק הישראלי, מידע שיש בו כדי לפגוע בביטחון המדינה וכיוצא בזה).

## 3. עקרונות וכללי אבטחת מידע

3.1. חובת אבטחת המידע וחובת הסודיות מהוות תנאי סף בלתי נפרד בהתקשרות.

3.2. הספק מאבטח את המידע בהתאם לסטנדרטים מקובלים והולמים את רמת הרגישות של המידע הסודי.

3.3. עם תחילת עבודתו של הספק או חשיפתו למערכות הב"ה באופן פיזי או לוגי הספק יתדרך את עובדיו בהתאם למדיניות הב"ה בנושאים הבאים: האיומים הרלוונטיים למערכת, הנזקים הפוטנציאליים מתקיפת סייבר של המערכת, פירוט ההנחיות בהן הם נדרשים לעמוד וליישם.

3.4. הספק מתחייב לסודיות מול הב"ה באופן אשר יחייב אותו ואת עובדיו.

3.5. הספק מתחייב למלא אחר כל הוראות אבטחת המידע לגבי שמירת מידע כפי שיועברו ע"י הנהלת בתי המשפט (להלן הב"ה).

3.6. הספק ידאג לאבטחת כל חומר שיגיע אליו במסגרת ביצוע התחייבויותיו על פי הסכם זה ויהיה אחראי כלפי הב"ה על כל המידע המועבר אליו או דרכו.

3.7. באחריות הספק לדאוג לחיסיון, אמינות וזמינות המידע של הב"ה שברשותו.

3.8. הספק יפריד את הפעילות המתבצעת עבור הב"ה מפעילויות עיבוד אחרות המבוצעות על ידו על-ידי הקמת סביבת עבודה ייעודית נפרדת עבור הב"ה. הפרדה לוגית תתקיים ברמת הרשתות ועוד וברמת המשאבים אשר מוקצאים להב"ה.

3.9. לספק ולעובדיו תהיה מחויבות לעמוד במדיניות ובדרישות אבטחת המידע, הגנת הסייבר והגנת הפרטיות אשר יוגדרו על ידי הב"ה.

3.10. המידע והנתונים המועברים ו/או הנשמרים ו/או המוצגים באמצעות מערכת הספק אינם קניינו, ואין לו כל זכות לצפות בהם ו/או להשתמש בהם שלא לצורך התקשרות זו.

3.11. הספק מנוע משימוש במידע הסודי לצורך פרסום ו/או טיוב נתונים ו/או כל שימוש אחר שאינו לצורך התקשרות זו. ככלל, אין אישור לפרסום פרטי ההתקשרות לגורמי צד ג'.

3.12. הספק מתחייב לשתף פעולה עם הב"ה בכל אירוע חריג בו מעורב עובד הספק, או שקיים חשד למעורבות שיש עמה השלכה ישירה או עקיפה על ביטחון מערכות המידע של הב"ה.

3.13. הספק יקיים בקפידה את כל דרישות הב"ה בתחום אבטחת המידע ובכלל זה דרישות הממונה על אבטחת המידע של הב"ה ומנהל הביטחון של הב"ה.

3.14. קיים איסור על הספק להעביר מידע לצד שלישי (צד ג') כלשהו שקיבל במסגרת ההתקשרות או להשתמש במידע שאליו נחשף אגב ביצוע ההתקשרות או לכל מטרה אחרת שלא קשורה ישירות לביצוע ההתקשרות.

3.15. הספק לא רשאי לעשות שימוש במידע המשויך להב"ה לשימושו וזאת ללא קבלת אישור רשמי מראש מהב"ה.

3.16. כל המידע, התוכנות, האפליקציות, הנתונים, קוד ועוד אשר יאוחסנו על ידי הספק לשם התקשרות זאת יהיו בבעלותה המלאה והבלעדית של הב"ה. הספק יצהיר כי הוא מוותר על זכותו לתבוע כל זכות קניינית מהב"ה, ובכלל זה את הזכות לקניין רוחני. למען הסר ספק, כל החומר המועבר על ידי הב"ה לספק וכל המידע הנצבר במערכות אשר לספק גישה אליהם הינו בבעלות הב"ה כולל זכויות הקניין חומרי ורוחני והינם בבעלותו הבלעדית ואין לספק כל זכות לתבוע שימוש במידע או לבצע בו כל שימוש שאינו באישור הב"ה.

3.17. הספק מתחייב מראש לחתום על הסכם סודיות (NDA) בו הספק מתחייב לשמור על סודיות המידע במסגרת ההתקשרות.

3.18. הספק לא מורשה לעשות שימוש בשירותי צד ג' כחלק ממתן השירות ללא אישור מראש ובכתב של הלקוח וידיעתו. במידה ואושר לספק להתקשר עם שירותי צד ג', באחריות הספק להחתים גם את הספקים הנוספים במתן שירותי צד ג על הדרישות להן הוא מחויב.

3.19. יש לפעול לצמצום מידע שנאסף, באחריות הספק למחוק נתונים או מידע עודף אשר נאספו ואינם הכרחיים או רלוונטיים או נדרשים לשם עמידה בהוראות הסכם זה.

3.20. הספק רשאי לגשת או לעבד רק מידע המשויך להב"ה שהנו למטרות ההתקשרות.

## 4. חובת דיווח

4.1. הספק מתחייב לדווח למזמין במיידית, במהלך כל שעות היממה, וללא שיהוי, על כל אירוע אבטחה או חשד לאירוע אבטחה אשר מסכן מידע או מערכות של המזמין או עלול להשפיע על הב"ה או על יכולתו לעמוד בהתחייבויותיו נשוא ההסכם, ובפרט יודיע למזמין על האירועים הבאים:

4.1.1. אירוע אבטחה או תקיפת סייבר אשר הביאו לדלף מידע הקשור למזמין או לשיבושו של מידע או קוד תוכנה או לפגיעה בזמינות המידע.

4.1.2. אירוע אבטחה או ניסיון תקיפת סייבר אשר עלול להביא לפגיעה במערכות המזמין, במערכות המסופקות לו, במידע של המזמין או בקוד המשמש אותו.

4.1.3. אירוע אבטחה או ניסיון תקיפת סייבר אשר מטרתו לאסוף מידע על המזמין.

4.2. במקרה כאמור, על הספק להודיע למזמין על התרחשות האירוע, על הפעולות ננקטה ועל כל פרט נוסף ביחס לאירוע זה. יודגש כי חובה זה תחול גם אם אין בידי הספק את כלל המידע הרלוונטי, ועליו יהיה לעדכן את דיווחיו בהתאם למידע שיצטבר אצלו ולהנחיות המזמין. על הדוח המתועד לכלול את הפרטים הבאים:

4.2.1. אופן הטיפול באירוע, ועל האמצעים הננקטים באופן מידי לצורך צמצום הנזק, ומזעור החשיפה בטווח הזמן המידי.

4.2.2. תיאור כללי של האירוע, ראיות שנאספו, ידע שנצבר לגבי האירוע, אופן התרחשותו, סקירת היסטוריית האירוע הידועה ועוד.

4.2.3. המערכות אשר נפגעו או היו היעד לתקיפה.

4.2.4. המידע אשר זלג, נפגע או שהיה היעד לתקיפה, לרבות בירור אפשרות לפריצה לנתונים פרטיים או חסויים או ניסיונות לפריצות אלו.

4.2.5. ניתוח דרכי התקיפה, החולשות ששימשו את התקיפה או חולשות שהתגלו, התובנות שנלמדו וכול מידע רלוונטי אחר.

4.2.6. פעולות שננקטו או פעולות מתקנות למניעת הישנות אירועים בעתיד.

4.2.7. כל מידע אחר שיידרש על ידי הב"ה לצורך ניתוח האירוע, השפעתו והצעדים הנדרשים בעקבותיו.

4.2.8. במידה ויידרש ולפי הצורך, הספק יעביר להב"ה ראיות רלוונטיות.

4.2.9. הספק יפעל להעברת דיווח סטאטוס טיפול באירוע ובסיום הטיפול יעביר להב"ה דוחות סיכום, לרבות מסקנות והפקת לקחים בעתיד בעקבות האירוע.

4.3. חובת הדיווח המפורטת תוגבל למידע הרלוונטי למערכות הספק המשמשות למתן שירותים למזמין, ולא נדרש גילוי מידע של לקוחות או גורמים בלתי קשורים אחרים.

4.4. הספק יחתים את גורמי שרשרת האספקה על התחייבות להודיע למזמין בהקדם האפשרי וללא שיהוי, על כל אירוע אבטחה, כמפורט מעלה, אשר מסכן מידע או מערכות של הספק או המזמין ואשר עלול להשפיע על יכולת הספק לעמוד בהתחייבויותיו לפי ההסכם. הודעה כאמור תהיה כמפורט מעלה.

4.5. הספק ידווח באופן מידי על כל אירוע אבטחה שפגע או עלול לפגוע במידע הסודי או על אירוע דליפת מידע ו/או חריגה מהרשאה שניתנה ו/או אירוע אבטחת מידע או אירוע אבטחה ועל כל הליך משפטי שהספק מעורב בו ושעלול להשפיע על המידע הסודי.

4.6. הספק יספק הקצאה של משאבים הולמים לניהול אירועי אבטחת מידע, המשאבים שיוקצאו על ידי הספק נדרשים להבטיח תגובה מהירה, אפקטיבית ומסודרת לאירוע האבטחה.

4.7. הספק נדרש לדווח, אחת לשנה לפחות, להב"ה על אודות אופן ביצוע חובותיו לפי מסמך זה.

4.8. באחריות הספק לדאוג לביטול ההרשאות של משתמש שסיים את תפקידו מיד עם סיום תפקידו ובנוסף עליו להודיע על כך במיידי להב"ה.

## 5. מתכנן סייבר

5.1. לטובת תכנון, פיקוח ובקרה על יישום המענה להגנת הסייבר, יעמיד המציע מתכנן סייבר אשר יאושר ע"י המזמינה ויעמוד בתנאי הסף הבאים:

5.2. ניסיון מוכח של 5 שנים בתכנון, ליווי ופיקוח על יישום פתרונות הגנת סייבר למערכות OT ו-IOT ובפרט מערכות ביטחון מתח נמוך ובקרת מבנה ב 10 השנים האחרונות.

5.3. ניסיון מוכח ב-2 פרויקטים מסוג זה בגופים ממשלתיים/ציבוריים.

5.4. מחזיק בהסמכה תקפה לאחד התארים הבאים:

5.4.1. CSSA - Certified SCADA Security Architect

5.4.2. CISSP - Certified Information Systems Security Professional

5.4.3. CISM - Certified Information Security Manager

5.4.4. CCSP – Certified Cyber Security Professional

5.5. חלה חובה למנות מתכנן אבטחת מידע מטעם הספק.

5.6. יש להבהיר שניתן למנות נציג מטעם הספק שיהיה מתכנן סייבר וזאת בנוסף על תפקיד אחר שבו הוא נושא ובתנאי שיהיה פנוי למלא את התפקיד באופן מלא.

5.7. המתכנן יוגדר כרפרנט אבטחת מידע על ידי הספק למול הפעילות הרלוונטית של הב"ה.

5.8. קורות חיים של המתכנן יצורפו במענה לפרק זה.

5.9. עד אישורו של המתכנן לתפקיד על ידי הב"ה, יחשב מנכ"ל הספק כבעל האחריות הכוללת לנושא.

5.10. להב"ה שמורה הזכות להתנגד לבחירתו של המועמד, וכן תעמוד בפניה הזכות לדרוש החלפתו בכל עת. על הספק למלא אחר ההוראה זו בתוך 10 ימים.

5.11. פרטיו ודרכי יצירת קשר ימסרו לארגון.

5.12. המתכנן יהיה פנוי וזמין לביצוע תפקידו.

5.13. הספק יעניק למתכנן סמכויות, כלים ואמצעים הנדרשים לביצוע תפקידו, לרבות סמכויות אכיפה על עובדי החברה בתחומי אבטחת מידע.

5.14. על המתכנן להיות בקיא בפרטי נספח זה ובשאר נהלי אבטחת המידע הרלוונטיים, החלים על הספק וכל מי מטעמו, ולאכוף אותם.

5.15. בין תפקידיו של המתכנן על אבטחת המידע:

5.15.1. הכנת נוהל אבטחת מידע ותכנית לבקרה שוטפת על העמידה בדרישות אבטחת המידע, הסייבר והפרטיות ויודיע להב"ה על ממצאים שהתגלו.

5.15.2. יישום מדיניות האבטחה לרבות אבטחה פיזית, וידוא זהות משתמשים, אבטחה בניהול כוח אם, בקרת גישה, ניהול הרשאות, הגנת חיבור התקנים, אבטחת תקשורת, ניהול ספקים ושרשרת אספקה, ניהול אירועי אבטחה, דיווח על אירועי אבטחה ועוד.

5.15.3. הקצאת משאבים הולמים הדרושים לאבטחת המידע, להגנת סייבר והגנת הפרטיות של פעילות הב"ה ושל ההתקשרות.

5.15.4. אחריות להיות בקשר שוטף עם נציגי אבטחת המידע והסייבר הארגון, בכל עת שיידרש לכך.

5.15.5. המתכנן יתדרך ויעדכן את עובדי הספק (וגורמי צד ג' במידה ונקבעו) בהוראות ובנהלים התקפים ואלה שיינתנו מפעם לפעם.

## 6. תפקידיו של מתכנן הסייבר

6.1. ליווי הפרויקט בכל תקופת ההתקשרות - תכנון, הקמה, בדיקות, הפעלה, תחזוקה ושירות.

6.2. גיבוש דרישות והנחיות לתכנון הפתרון להגנת הסייבר ואבטחת המידע בכל תקופת ההתקשרות.

6.3. ביצוע סקר סיכוני הסייבר ואבטחת המידע על הפרויקט.

6.4. הנחיה ופיקוח, לרבות פרסום הנחיות בשלבים השונים של תקופת ההתקשרות.

6.5. ביצוע בדיקות להגנת הסייבר (ATP), אחריות לתיקון הליקויים ככול שיתגלו ודיווח לגורמים השונים (לרבות למזמין).

6.6. הדרכת הצוותים בתפעול מערכות הגנת הסייבר, בדגש על תרגול השימוש במערכת ניטור הסייבר.

6.7. הכנת נוהל אבטחת מידע ותכנית לבקרה שוטפת על העמידה בדרישות אבטחת המידע, הסייבר והפרטיות ויודיע להב"ה על ממצאים שהתגלו.

6.8. כתיבה ויישום מדיניות הגנה פיזית וסביבתית .המדיניות תכלול מדיניות ומשאבים מתאימים לארגון, כגון נעילת משרדים בסוף יום, מצלמות אבטחה, מידור, כניסת אורחים וכניסת עובדים חיצוניים למתחמי החברה ולאזורים רגישים והגנה נאותה על חדרי השרתים וחדרי הבקרה.

6.9. הקצאת משאבים הולמים הדרושים לאבטחת המידע, להגנת סייבר והגנת הפרטיות.

## 7. שרשרת אספקה

7.1. דרישות התקשרות לרבות דרישות אבטחת המידע המפורטות להלן, חלות על כול גורמי שרשרת האספקה של הספק, לרבות גורמי צד ג'/צד שלישי (במידה ואושרו מבעוד מועד על ידי הב"ה).

7.2. הספק יפקח, יסקר ויבקר באופן סדיר אחר הגורמים שלו בשרשרת האספקה, לרבות ניטור וסקירה של צד ג' (צד שלישי).

7.3. על הספק מוטלת האחריות לוודא כי גורמי צד ג' או ספקי משנה שלו מיישמים באופן מלא את תנאי ההתקשרות ועומדים בדרישות שהוגדרו.

7.4. על הספק למנות גורם אחראי לתחום שרשרת האספקה. הגורם האחראי בתחום שרשרת אספקה יוודא הקצאת משאבים הולמים וירכז את המענה בכדי לתת מענה לאיומים הנובעים מחולשות אפשריות בשרשרת האספקה.

7.5. ספק יאפשר ביצוע ביקורות חיצוניות מטעם המזמינה בהקשר לעמידה בדרישות ההתקשרות ועמידה בדרישות אבטחת המידע, לרבות סקר ספקים וסקר שרשרת אספקה.

7.6. הספק יחתים את גורמי שרשרת האספקה (אשר הורשו מראש על ידי הב"ה) על התחייבות להודיע למזמין בהקדם האפשרי וללא שיהוי, על כל אירוע אבטחה, כמפורט מעלה, אשר מסכן מידע או מערכות של הספק או המזמין ואשר עלול להשפיע על יכולת הספק לעמוד בהתחייבויותיו לפי ההסכם.

7.7. הספק יהיה ערוך לתפעל אירועי אבטחת מידע הנובעים מליקויים בשרשרת האספקה ברמה חוזית, תהליכית וטכנולוגית.

## 8. שימוש בכלי AI בינה מלאכותית

8.1. שימוש בבינה מלאכותית בהתאם לדין- הספק מצהיר ומתחייב כי כל שימוש בטכנולוגיות בינה מלאכותית במסגרת השירותים ייעשה בהתאם להוראת ההסכם, לדין החל ולהנחיות המזמין ולמטרות שהוגדרו בלבד.

8.2. אישור מראש ובכתב לשימוש בבינה מלאכותית- הספק מתחייב כי לא יעשה כל שימוש בטכנולוגיות בינה מלאכותית במסגרת מתן השירותים, אלא לאחר קבלת אישור מפורש, מראש ובכתב, מאת המזמין, ובהתאם לתנאים שייקבעו באישור זה.

8.3. תחולת האישור והגבלת מטרות- אישור שניתן לשימוש בבינה מלאכותית יחול אך ורק על המטרות, ההיקף, הכלים והתקופה שצוינו במפורש באישור, ולא יפורש כהיתר כללי או מתמשך.

8.4. איסור העלאת חומרים לכלי בינה מלאכותית- ללא קבלת אישור מראש ובכתב מאת המזמין, נאסר על הספק להעלות, להזין או למסור לכלי בינה מלאכותית מכל סוג שהוא, לרבות כלים חיצוניים או צד ג', האיסור תקף לגבי כל מסמך, קובץ, תמונה, הקלטה, וידאו, מידע, נתון או תוכן אחר השייך למזמין או הקשור לשירותים הנדרשים ממנו.

8.5. שקיפות וגילוי- הספק ימסור למזמין מידע מלא ומדויק בדבר סוגי כלי הבינה המלאכותית בהם יעשה שימוש (במידה ואושרו), אופן פעולתם, מטרת השימוש, ורמת המעורבות האנושית בתהליך.

8.6. בעלות על מידע ותוצרים- כל מידע, נתון או חומר המסופקים על ידי המזמין יישארו בבעלותו הבלעדית. תוצרים שנוצרו באמצעות בינה מלאכותית במסגרת השירותים ייחשבו כתוצרי הספקה ויוקנו למזמין, אלא אם הוסכם אחרת בכתב.

8.7. מיקום גאוגרפי של השימוש והעיבוד- הספק מתחייב כי כל שימוש בבינה מלאכותית (במידה ואושר), לרבות עיבוד, אחסון, העברה או ניתוח של מידע הקשור לשירותים, ייעשה אך ורק בתחומי מדינת ישראל ובאישור מיוחד, במדינות האיחוד האירופי. חל איסור מוחלט על עיבוד, אחסון או שימוש במידע באמצעות כלי בינה מלאכותית המופעלים, מתארחים או מנוהלים מחוץ לישראל או לאיחוד האירופי.

8.8. איסור אימון ושימוש משני- הספק לא יעשה שימוש במידע של המזמין לצורך אימון, שיפור, כיול או פיתוח של מערכות בינה מלאכותית, ולא יעשה בו שימוש חוזר לכל מטרה אחרת, אלא אם ניתנה לכך הסכמה מפורשת מראש ובכתב.

8.9. הגנת מידע ואבטחתו- הספק מתחייב ליישם אמצעי אבטחת מידע הולמים לשם הגנה על המידע של המזמין (במידה ואושר), ולמנוע גישה בלתי מורשית, דליפה או שימוש חורג, לרבות במסגרת שימוש מאושר בבינה מלאכותית.

8.10. איכות, דיוק ואמינות התוצרים- הספק אחראי לכך שתוצרי הבינה המלאכותית יהיו מדויקים, סבירים ומתאימים לדרישות ההסכם, ויבצע בקרות נדרשות לצמצום טעויות, כשלים או מידע שגוי.

8.11. אחריות והיעדר פטור- השימוש בבינה מלאכותית לא יגרע מאחריות הספק על פי ההסכם או על פי דין. הספק לא יטען לפטור, הקלה או צמצום אחריות בשל שימוש בכלי אוטומטי.

8.12. זכות בקרה וביקורת- למזמין תעמוד הזכות לדרוש מידע, מסמכים והבהרות בנוגע לשימוש בבינה מלאכותית, וכן לבצע בקרה סבירה על עמידת הספק בהוראות סעיף זה.

8.13. דיווח על אירועים וחריגות- הספק יודיע למזמין ללא דיחוי על כל אירוע חריג, טעות מהותית, חשד לפגיעה במידע, או שימוש בבינה מלאכותית בניגוד לאישור שניתן או להוראות ההסכם.

8.14. הפסקת שימוש וסיום התקשרות- עם סיום ההתקשרות, או לפי דרישת המזמין, יפסיק הספק כל שימוש בבינה מלאכותית הקשור לשירותים או למידע המזמין, ימחק או ישיב את כלל הנתונים, ויאשר בכתב את ביצוע האמור.

## 9. נהלים

9.1. הספק יידרש להכין בתקופת ההקמה, המעבר ובמידה ובוצע שינוי משמעותי, נהלי תפעול לאבטחת מידע אשר יאושרו ע"י הב"ה. הספק יידרש ליישם את נהלי תפעול אבטחת המידע שלו, להתאימם לצרכי הב"ה ולהגישם לאישור הב"ה. לאחר קבלת האישור, על הספק לפעול לפי נהלים אלו.

9.2. לבקשת הב"ה, הנהלים יופצו ע"י הספק לגורמים הרלוונטיים.

## 10. דרישות אבטחת מידע

10.1. אבטחה פיזית וסביבתית

10.1.1. הספק יבטיח שהמערכות המשמשות לאספקת שירות ותוצרים להב"ה, יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה (מניעת גישה מגורמים בלתי מורשים) והתואם את אופי הפעילות ורגישות המידע בו. בנוסף יש למנוע יכולת צפייה של גורם בלתי מורשה במערכות ובנתונים (כגון דרך חלון או דלת).

10.1.2. הספק ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויות המערכות המספקות שירות ותוצרים להב"ה.

10.1.3. הספק אחראי להבטיח הגנה פיזית נאותה על חדרי התקשורת, ארונות תקשורת וציוד נלווה, במטרה למנוע חדירה, גישה או שימוש בלתי מורשים. במסגרת זו יותקנו אמצעי בקרת כניסה מתאימים, לרבות קודנים או אמצעים מקבילים, בהתאם להנחיות המזמין. בנוסף, תוגדר ותופעל מערכת התרעה על מצב של דלת מוטרדת או דלת פתוחה שלא

כדין, הכוללת חיווי מקומי ו או דיווח למערכת מרכזית, לפי הצורך. כלל האמצעים יתוחזקו במצב תקין לאורך כל תקופת ההתקשרות ועל חשבון הספק.

10.1.4. יש להפריד בין המערכות המשמשות את הב"ה לבין מערכות המשמשות גורמים אחרים.

10.2. זיהוי ואימות

10.2.1. אופן הזיהוי של משתמש ארגוני במערכת ארגונית פנימית יעשה תוך הסתמכות על מנגנון אימות זהות של המשתמש מבוסס על Active Directory (ככלל יעשה שימוש במנגנון זה, אלא אם כן לא ניתן לעשות זאת במערכת הייעודית).

10.2.2. אופן הזיהוי יעשה ככול האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המשתמש המורשה.

10.2.3. אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, במידה ולא ניתן להשתמש באמצעי פיזי- מאושר לעשות שימוש מבוסס על סיסמאות (14 תווים לפחות) עם מרכיב אימות הזדהות נוסף (כגון OTP). השימוש בסיסמה מאושר בתנאי שאורך הסיסמה והמורכבות יהיו בתצורה מקובלת ועדכנית ובהתאמה לרגישות המידע, תבוצע נעילה לאחר לא יותר מ 5 ניסיונות שגויים ותבוצע החלפת סיסמאות מדי שישה חודשים לפחות..

10.2.4. משתמש ינותק או הגישה שלו תינעל לאחר פרק זמן סביר של אי-פעילות.

10.2.5. הגישה למערכת ולנתונים תיעשה בידי בעל הרשאה המורשה לכך בלבד.

10.2.6. לא יעשה שימוש בסיסמאות ברירת מחדל או סיסמאות זהות באתרים או בשירותים שונים.

10.2.7. זיהוי ואימות של משתמש חיצוני יבוצע על ידי מערכת ההזדהות הממשלתית או כרטיס חכם או מערכת IDP.

10.2.8. סיסמאות ברירות מחדל יוחלפו במיידי ובפרט לממשקי ניהול, ציוד תקשורת ושרתים.

10.3. ניהול הרשאות גישה

10.3.1. יינתנו הרשאות בהתאם להגדרות תפקיד, הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.

10.3.2. הגישה תסופק רק לבעלי הרשאה תקפה.

10.3.3. נדרש ביטול ההרשאות במיידי לגורם אשר שסיים את תפקידו.

10.4. תיעוד של אירועי אבטחה (אבטחת מידע), רישום לוגים וניטורם לרבות בקרה ותיעוד גישה של נתונים פרטיים של הב"ה או מידע מסווג

10.4.1. ינוהל מנגנון תיעוד אוטומטי (לוגים) שיאפשר ביקורת על הגישה למערכות המאגר המכילות נתונים פרטיים או מידע של הב"ה או מידע מסווג ובכלל זה נתונים אלו: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

10.4.2. מנגנון ניהול התיעוד האוטומטי יפעל באופן קבוע, יסייע לאיתור אירועים ויפיץ התרעות לאחראים.

10.4.3. אין להשתמש במערכת ללא לוג. במידה ונדרש להשתמש במערכת ללא לוג, הנושא יועבר לבחינה של הממונה על אבטחת המידע לקביעת החלטה בנושא.

10.4.4. יש לדאוג ליידוע בעלי ההרשאות בדבר קיום מנגנון הבקרה והתיעוד האוטומטי.

10.4.5. יש לשמור את נתוני תיעוד אירוע האבטחה לתקופה של 24 חודשים או לחילופין להעבירם לשרת ניהול לוגים מרכזי שאושר מבעוד מועד על ידי הב"ה.

10.4.6. יש לתעד כל כניסה לממשקי הניהול של האפליקציה, כל שינוי שהתרחש באפליקציה וכול פעילות של משתמשים לרבות מנהלי הרשת, המפעילים של ה SOC וצוות אבטחת המידע.

10.4.7. בעת חשיפת הלוגים הספק יבטיח שרק להב"ה תהיה גישה לרשומות הנוגעות לפעילותה.

10.4.8. יתקיים סנכרון שעונים NTP עם מקור זמן מדויק ומוסכם.

10.4.9. נהלים של ניהול הלוגים יהיו זמינים להב"ה.

10.5. אבטחת עמדות הקצה

10.5.1. חל איסור מוחלט לשמור מידע רגיש בתחנה של המשתמש שלא הותאמה למדיניות מסמך זה.

10.5.2. מחשבי הספק מהם ניתן לגשת למידע של הב"ה ולמערכותיה, יצוידו במערכת הפעלה ובתוכנות EDR/XDR (אנטי וירוס מתקדם) מעודכנות.

10.5.3. הסביבה שתוגדר לצורך טיפול במידע של הב"ה תופרד מסביבת העבודה של הספק באמצעות אמצעים לוגיים (כגון Firewall וסגמנטציה).

10.5.4. יוטלו הגבלות על התקנת תוכנות בתחנות העבודה.

10.5.5. דוחות אירועי מערכת של תחנות העבודה יועברו למערכות הניטור של הספק.

10.5.6. החיבור אל מערכות המידע של הב"ה יהיה בהתאם להנחיות הב"ה.

10.6. התקנים ניידים

10.6.1. הספק מתחייב שלא להוציא מידע להתקנים ניידים.

10.6.2. יש להגביל אפשרות לחיבור התקנים ניידים למערכת.

10.6.3. במידה ונדרש מהספק לצורך פעילותו לעשות שימוש בהתקן נייד, מתחייב הספק לפנות מבעוד מועד לקבלת אישור מראש מהב"ה וכן לנקוט באמצעי הגנה נאותים שיונחו על ידי הב"ה וזאת על מנת להבטיח את שלמות , סודיות וזמינות המידע.

10.6.4. בשימוש בהתקן נייד הנדרש לביצוע ההסכם ואושר מראש על ידי הב"ה בהתאמה לסיכונים ולרגישות המידע, הספק מחויב לעשות שימוש בשיטות הצפנה מקובלות אשר ייחשבו כאמצעי סביר להגנה על המידע.

10.7. יש למנוע שינוי הגדרות BIOS או EUFI על ידי גורם בלתי מורשה באמצעות הגדרת סיסמה.

10.8. הצפנת מידע

10.8.1. נדרשת הצפנה מלאה של דיסק ברמה מקובלת של מחשבים ניידים ונתונים שבהם קיים מידע של הב"ה או מידע פרטי או רגיש.

10.8.2. נדרשת הצפנה של התקנים בהם קיים מידע של הב"ה או מידע פרטי או רגיש (לפחות ברמה של AES 256). יש להדגיש שיש לקבל אישור מבעוד מועד מהב"ה לשימוש בהתקן נייד.

10.9. אבטחת התקשורת

10.9.1. הב"ה עושה שימוש ברשת תקשורת משרדית קווית (חוטית). אין לעשות שימוש בתקשורת אלחוטית כגון Wi-Fi.

10.9.2. קיימת הפרדה בין רשתות המאכלסות את מאגרי המידע של הב"ה, יישומים, תחנות עבודה של המשתמשים וכלל הרשתות האחרות. אין לחבר רשתות שונות כגון רשת מערכות מידע, בקרת מבנה או מערכות ביטחון ועוד בינן לבין עצמן- כל רשת הנה נפרדת ותוגן על-ידי הפרדת פיזית או על ידי חציצה חזקה.

10.9.3. הספק מתחייב כי מערכות ומאגרי המידע של הב"ה לא יחוברו לסביבת האינטרנט, אלא אם כן קיבל את אישור הב"ה לכך. במידה וקיבל הספק אישור וחיבר את המערכות ו/או מאגרי המידע לרשת ציבורית או לאינטרנט, מתחייב הספק לנקוט באמצעי ההגנה המתאימים על מנת למנוע נזק, פריצה, זיהום או השחתה של מאגרי המידע. תצורת החיבור במידה ותאושר, נדרשת לקבל אישור רשמי ובכתב של הב"ה.

10.9.4. במידה ואושר מראש ובכתב חיבור לתקשורת מול רשת ציבורית או אינטרנט של שירות או שרת המכיל מידע מסווג או פרטי , יש להתקין אמצעי הגנה מתאימים המונעים חדירה לא מורשית ומגנים בצורה הולמת מפני קוד זדוני (איום של וירוס).

10.9.5. יש להגדיר כתובות ידניות לרכיבי התקשורת המרכזיים (לא DHCP).

10.9.6. ככלל, תעבורת תקשורת או גישה או העברת מידע ברשת הפנימית של הב"ה, תיעשה תוך שימוש בשיטות הצפנה מקובלות.

10.9.7. גישה או העברת נתונים או מידע של הב"ה ברשת ציבורית או באינטרנט או בקווי תקשורת אל הב"ה או בתקשורת מהב"ה (אשר אושרה מראש) תיעשה תוך שימוש בשיטות הצפנה מקובלות.

10.9.8. גישה לניהול המערכת תבוצע אך ורק מהרשת הארגונית של הב"ה (ולא תבוצע מרשת אינטרנט או מרשת ציבורית).

10.9.9. על ציוד המשמש להעברת תקשורת (כגון: מתגים, נתבים, Firewall ועוד) לעבור הקשחה בהתאם למדיניות היצרן לרבות עדכוני Firmware.

10.9.10. אין אישור לחבר רכיב מחשוב או רכיב תקשורת לרשת הב"ה. במידה וקיים צורך יש לקבל על כך אישור מראש מהב"ה. חיבור בלתי מורשה מהווה הפרה יסודית של ההתקשרות.

10.10. גישה מרחוק

10.10.1. גישה מרחוק מרשת ציבורית או מהאינטרנט מחייבת אישור מראש של הנהלת בתי המשפט, ככלל לא מאושרת גישה זאת.

10.10.2. לא יאושר חיבור לרשת ציבורית או מהאינטרנט בלא התקנת אמצעי הגנה מתאימים המונעים חדירה לא מורשית ומגנים בצורה הולמת מפני קוד זדוני.

10.10.3. גישה או העברת מידע ברשת ציבורית או באינטרנט (אשר אושרה מראש), תיעשה תוך שימוש בשיטות הצפנה מקובלות.

10.10.4. גישה מרחוק (במידה ותאושר על ידי הב"ה מראש) מחייבת בנוסף גם שימוש באמצעי נוסף שמטרתו לזהות את המתקשר והמאמת את הרשאתו לביצוע הפעילות מרחוק (כגון בנוסף עוד אמצעי כגון סיסמה חד פעמית OTP).

10.11. ממשקים מאובטחים

10.11.1. יש להגביל גישה לממשקים לרבות הגדרתם לשימוש הייעודי המתוכנן בלבד לרבות הגדרת גישה רק מרשתות מורשות לכך ובתצורה גישה מקובלת ומאושרת.

10.11.2. יש לדאוג לחסום את הגישה לממשקי הניהול של האפליקציה מפני גורמים לא מורשים. יש למנוע התחזות למערכת.

10.11.3. יש להגן על המידע העובר בין ממשקים לרבות מפני יירוט או ציטוט, שימוש בהצפנה מקובלת יהווה פתרון מקובל.

10.12. גיבוי ושחזור

10.12.1. הספק נדרש לפתרון לגיבוי של המערכת ושל המידע והנתונים.

10.12.2. רמת האבטחה של הגיבוי תהיה באותה רמת אבטחה של השימוש.

10.12.3. הספק אחראי לשמור ולגבות גם אירועי אבטחה בהתאם לדרישות החוק, התקנות וההתקשרות.

10.12.4. יש לקבוע נהלים לביצוע גיבוי ולהבטחת השחזור ובתנאי שהשחזור מאושר על ידי הב"ה.

10.12.5. לספק קיימים נהלים לשחזור מידע לשם עמידה בדרישות ההתקשרות.

10.12.6. הספק יאחסן את הגיבוי בצורה מוגנת ומאובטחת (פיזית ולוגית) אשר תבטיח את שלמות המידע ויבטיחו את אפשרות שחזור המידע במקרה של אבדן או הרס.

10.12.7. הספק מתחייב לבצע שחזורים מדגמיים של המדיות המגבות על תשתיותיו לצורך בדיקת התאוששות. בסיום השחזור המדגמי מתחייב הספק למחוק את המידע ששוחזר.

10.12.8. הספק מתחייב כי שחזור יבוצע אך ורק באישור הב"ה.

10.12.9. הספק מתחייב כי במידה ובוצע שחזור יתועדו כל הליכי השחזור כולל זהותו של מבצע השחזור ופרטי המידע ששוחזר.

10.13. שימוש בחומרה, בתוכנות לרבות רישיונות, עדכונים והגנת קוד זדוני

10.13.1. ייעשה שימוש רק בחומרה אשר נתמכת על ידי היצרן וזאת תחת אחריות, שירות ותחזוקה, לרבות עמידה בדרישות מומלצות של היצרן.

10.13.2. הספק מחויב לפעול עם חומרה העומדת בדרישות מומלצות מטעם היצרן.

10.13.3. הספק מחויב להתקין תוכנות מורשות, חוקיות ובעלות רישיון תקף בלבד.

10.13.4. מערכות ההפעלה והתוכנות אשר ישמשו את המערכת יתמכו על ידי היצרנים.

10.13.5. ייעשה שימוש רק במערכות ובתוכנות שהיצרן תומך בגרסאות שלהן.

10.13.6. לא יעשה שימוש בתוכנות הכוללות פגיעויות/חולשות קריטיות או גבוהות ידועות. במידה ותתגלה פגיעות קריטית או גבוהה באחריות הספק לספק מענה בפרק זמן קצר ככל הניתן.

10.13.7. עדכוני אבטחה (Patches) יוטמעו בהתאם להמלצת היצרן.

10.13.8. ככלל, אם היצרן איננו ממשיך לספק עדכוני/תיקוני אבטחה (כגון End of support), אז המוצר לא מאושר לרכישה או לשימוש ברשת הב"ה. במידה ויש כוונה להפסקת עדכוני אבטחה מטעם היצרן יש לדווח על כך במידי להב"ה ולפעול להחלפת הפתרון.

10.13.9. יסופק מנגנון הגנה כנגד קוד זדוני או לגרום נזק או שיבוש למחשב או לחומר מחשב או לשרתים (כגון פתרונות כגון אנטי וירוס או EDR/XDR), המנגנון יעודכן באופן תדיר למול איומים חדשים.

10.14. יסופק מנגנון הגנה כנגד קוד זדוני או לגרום נזק או שיבוש למחשב או לחומר מחשב או לשרתים (כגון פתרונות כגון אנטי וירוס או EDR/XDR), המנגנון יעודכן באופן תדיר למול איומים חדשים.

10.15. בקרה ותיעוד גישה ונתוני אבטחה למידע פרטי או מידע של הב"ה או מידע מסווג

10.15.1. ינוהל מנגנון תיעוד אוטומטי (לוגים) שיאפשר ביקורת על הגישה למערכות המאגר המכילות מידע פרטי או מידע של הב"ה או מידע מסווג ובכלל זה נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

10.15.2. מנגנון ניהול התיעוד האוטומטי יפעל באופן קבוע, יסייע לאיתור אירועים ויפיץ התרעות לאחראים.

10.15.3. יש לדאוג ליידוע בעלי ההרשאות בדבר קיום מנגנון הבקרה והתיעוד האוטומטי.

10.15.4. יש לשמור את נתוני הבקרה, התיעוד של הגישה ונתוני האבטחה ל6 חודשים לפחות או לתקופה של 24 חודשים במידה ומדובר בנתונים הכוללים מידע פרטי או לחילופין יש להעביר את הלוגים למערכת SIEM מרכזית של הב"ה או לשרת ניהול לוגים שאושר מבעוד מועד על ידי הב"ה.

10.15.5. יש לתעד כל כניסה לממשקי הניהול של האפליקציה וכל שינוי שהתרחש באפליקציה.

10.16. הקשחות

10.16.1. המערכת ומרכיביה הפיזיים והלוגיים יעמדו במדיניות הקשחות מומלצת של היצרן.

10.16.2. יש להסיר שירותים מיותרים, פרוטוקולים פגיעים, ממשקים שאינם בשימוש וכל תוכנה או שירות שלא נדרשים לשם תפקוד המערכת.

10.16.3. יש להתקין פתרון הגנה כנגד קוד זדוני.

10.16.4. יש להצפין את הדיסקים הקשיחים היכן שמצוי מידע חסוי, רגיש או פרטי.

10.17. יש להגיש תיק תיעוד מערכת.

## 11. שימוש ב"ענן"

11.1. ככלל, אין אישור לשימוש במערכות "ענן", למעט חריגים בסמכות ובאישור בלעדי של הב"ה.

## 12. ביקורות לפי דרישה

12.1. הב"ה רשאית לבצע ביקורת לפי דרישה או בעקבות חשש לתקיפת סייבר או תקיפת סייבר המשפיעה על אספקת השירותים או המוצרים עבור הב"ה.

12.2. הביקורת תבוצע על ידי הב"ה או על ידי גורם שאותו היא הסמיכה לביצוע הביקורת מטעמה.

12.3. הספק מאשר מראש להב"ה או גורם צד ג' מטעם הב"ה לבצע ביקורת פתע, וזאת רק לפעילות הקשורה אודות הסכם זה בלבד.

12.4. הספק יאפשר ביצוע ביקורות חיצוניות מטעם המזמינה בהקשר לעמידה בדרישות ההתקשרות ועמידה בדרישות אבטחת המידע, לרבות סקר ספקים וסקר שרשרת אספקה. הב"ה יהיו רשאים לבצע בדיקות מערכי אבטחה, לרבות ניהולי וטכני, כולל איתור פרצות אבטחה, בדיקת עמידה בדרישות הגנת פרטיות ובדיקות יעילותם של מנגנונים ושל מערכות.

12.5. הב"ה רשאית לדרוש מהספק כי יבצע בדיקה או פעולה במערכותיו המשמשות למתן השירותים לצורך בחינת חשד לתקיפת סייבר או תקיפת אבטחת מידע וזאת על מנת לוודא כי לא מתקיים אירוע כאמור.

12.6. הספק ישתף פעולה כמיטב יכולתו עם דרישות המזמין ויעמיד לרשותו כל מידע נדרש לצורך אבחון והתמודדות עם אירוע האבטחה או לוודא כי אירוע כאמור לא מתקיים. מידע זה יוגבל למידע הרלוונטי למערכות המזמין או המערכות המשמשות למתן שירותים למזמין, וללא גילוי מידע של לקוחות או גורמים בלתי קשורים אחרים.

12.7. כל מידע שיועבר לספק לצורך בדיקה זו הוא רגיש ואין להעבירו לכל גורם אחר ללא אישור המזמין.
12.8. הספק יפעל ליישום המלצות הביקורת ולתיקון הליקויים, תוך פרק זמן סביר וללא עלות נוספת, כפי שייקבע על ידי הב"ה.
12.9. הספק יפעיל מערכת ביקורת פנים משלו.

## 13. מבדקי חדירה וסקרי סיכונים

13.1. מטרת מבדקים וסקרים הנה לוודא את התאמה לדרישות חוק, לתקנים, למדיניות ולנהלי הב"ה ולעמידה בדרישות אבטחת המידע, הסייבר והגנת הפרטיות.

13.2. הספק יערוך מבדק חדירות/בדיקת חוסן טכנולוגיות למערכת לבחינת עמידותה בפני סיכוני פנימיים וחיצוניים על חשבונו לפני הכנסתה למבצעיות וכן אחת לשמונה עשר חודשים לפחות.

13.3. בדיקת החדירה תבוצע באחריותו של הספק באמצעות גורם צד ג' בלתי תלוי. מבדק לא תלוי יכול לספק את הב"ה אם יתקבל מידע בשקיפות מספקת וזה יאושר מראש על ידי הממונה על אבטחת מידע בהב"ה.

13.4. ממצאי מבדק החדירות יועבר לעיון הב"ה.

13.5. הספק יפעל לתיקון הליקויים, ככול שהתגלו.

13.6. לפי דרישה ולפי הצורך יתקיימו מבדקים או סקרים חוזרים לווידוא שהממצאים טופלו כנדרש וזאת לפי שיקול דעת בתי המשפט.

13.7. כאשר לא ניתן לבצע מבדק או סקר, על הספק להעביר להב"ה עדויות על יישום דרישות אבטחת מידע, הגנת סייבר והגנת הפרטיות.

13.8. גרסה עם פגיעות קריטית או גבוהה לא תעלה לסביבה מבצעית (עלייה לאוויר), אלא אם כן הנושא אושר באופן רשמי על ידי הממונה על אבטחת מידע או מנהל אגף טכנולוגיות דיגיטליות ומידע מהב"ה.

13.9. הב"ה רשאית, מעת לעת וללא כל הודעה מוקדמת, לבצע סקרי סיכונים או מבחני חדירה בעצמה או על ידי חברה חיצונית שנמצאת בהתקשרות מטעמה והספק מחויב לשתף פעולה באופן מלא בביצוע הבדיקה ולתקן את הליקויים הגבוהים והקריטיים שיתגלו.

## 14. אישורי בטחון ומהימנות עובדים

14.1. הספק מתחייב כי כל עובדיו ו/או מי מטעמו אשר יהיו בעלי גישה למאגרי הב"ה ו/או יועסקו במסגרת התקשרות הספק עם הב"ה, יעמדו בתנאי סף לגבי רמת אמינות עובדים והעבר של עבירות הקשורות בשימוש במידע בהתאם לרגישות המידע וכן יהיו בעלי הכשרה מתאימה בהתאם לנדרש במסמכי המכרז וההתקשרות. בדיקת אימות הרקע של כל מועמד להעסקה כעובד הספק, מי מטעמו או משתמש צד שלישי, יעשו ע"י הספק כנדרש על פי דין ולפי כללי האתיקה הרלוונטיים, והיקפם יתאים לדרישות הב"ה, לסיווג המידע שיהיה נגיש להם ולסיכונים הצפויים.

14.2. הספק יעסיק בכל העבודות הקשורות בביצוע ההתקשרות אך ורק עובדים שאושרו להעסקה על ידי המזמין ולא יעסיק במתן השירותים הנדרשים עובדים מטעמו שטרם אושרו, לא יחשוף בפניהם כל חומר הקשור לביצוע הסכם זה בטרם קבלת האישור כאמור.

14.3. קבלת אישור מטעם המזמין להעסקת עובד ספק הנו עבור ההתקשרות הנ"ל שעבורה התקבל ההכשר ולא מהווה אישור אוטומטי לשיתופו בהתקשרות אחרת.

14.4. הספק לא יאפשר גישה לאתרים בהם יעבוד, לגורמים שאינם מוסמכים לכך

14.5. הספק מתחייב לעדכן את הרשימה של העובדים מטעמו (ועובדי צד ג' במידה ואושרו) בכל עת שיחולו בה שינויים, לרבות דיווח על עזיבת עובד באופן מיידי.

14.6. הספק יהיה אחראי כלפי הב"ה על כל פעילות עובדיו ו/או מי מטעמו במסגרת ההתקשרות.

14.7. הספק מתחייב שכל עובדיו, ו/או מי מטעמו ו/או משתמשי צד שלישי, מבינים את מלוא האחריות המוטלת עליהם בנוגע למידע ולאבטחתו וכי הם מתאימים לתפקידים שנועדו להם. על הספק להפחית סיכוני גניבה, הונאה או שימוש לרעה בגישה למידע של הב"ה באמצעות נקיטת אמצעי הגנה סבירים ומקובלים (כגון מצלמות אבטחה, תיעוד גישה וכדומה) וזאת מבלי לגרוע מהוראות נספח זה באשר לאבטחה הפיזית והסביבתית.

14.8. הספק יחתים את עובדיו, ו/או מי מטעמו ו/או משתמשי צד שלישי, על הסכם סודיות הנוגע לפעילות של הב"ה ואודות התקשרות זאת, הסכם הסודיות יהיה ללא פגות תוקף. בעת עזיבת עובד או מי מטעמו או משתמש צד שלישי באחריות הספק להזכיר לאותו גורם אודות התחייבות לסודיות ללא פגות תוקף שחתם והתחייב עליה.

14.9. בטרם יקבל הספק (או עובדיו) גישה למידע ממאגר המידע של הב"ה (באופן פיזי או לוגי), הספק יתדרך את עובדיו בנושא החובות לפי החוק והתקנות (הגנת פרטיות) וימסור להם מידע אודות חובותיהם לפי החוק, מדיניות האבטחה, נהלי האבטחה והוראות הסכם זה של הב"ה, יקיים הדרכות ריענון אחת לשנתיים לפחות או בזמן כניסה לתפקיד של עובד במסגרת הסכם זה או שינוי היקף הרשאותיו של העובד.

14.10. מנהל אגף הביטחון של הב"ה ו/או נציג אחר מטעם הב"ה יהיו רשאים לדרוש מהספק שלא לאפשר עבודה במסגרת הסכם התקשרות זה של מי מעובדיו, גם לאחר שהחל את עבודתו מול הב"ה, מבלי שיתנו טעם לכך והספק מתחייב מראש להרחיק את העובד מייד מהשתתפות ביישום הסכם זה אחר שיידרש לעשות זאת. הב"ה לא יהיה חייב לפצות את הספק בגין דרישה זאת.

14.11. הספק מצהיר בזה כי ידוע לו שכל הידיעות אשר בידו ו/או אשר תגענה לידו ו/או לעובדיו תוך כדי מימוש התחייבויותיו במכרז זה ו/או בקשר עמו, הינן חסויות והוא מתחייב לשמור על כל מידע לשם ביצוע הפרויקט ו/או בקשר עמו. אין לפרסמן בכל הקשר או למסרן לצד שלישי ללא קבלת אישור מראש ובכתב מהב"ה.

14.12. חוזה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי אבטחת מידע, וילווה בהצהרת סודיות.

14.13. הספק חייב להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם וליישם את אמצעי האבטחה הקבועים בהסכם.

14.14. במידה והתירה בכתב הב"ה לספק החיצוני לתת את השירות באמצעות גורם נוסף – הספק חייב לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו לרבות בדיקות המבוצעות בתהליכי גיוס העובדים. אבטחת מידע בעת העסקת עובדים, הגברת המודעות שלהם נוהלי אבטחת מידע והחתמה על התחייבות לשמור על סודיות המידע , להשתמש במידע רק לפי האמור בהסכם וליישם את אמצעי האבטחה הקבועים בהסכם.

14.15. לעובדים (כולל עובדים חיצוניים לארגון) המסיימים את העסקתם בארגון, בין אם ביוזמתם או ביוזמת המעסיק, ייחסמו הרשאות הגישה למידע (בין אם למערכות מידע ובין אם לאמצעים פיזיים.

14.16. הספק יוודא כי בסיום ההעסקה לא יישארו נכסי מידע של הארגון בידי העובד.

## 15. ספקי משנה ומיקור חוץ

15.1. הספק יקבל מראש ובכתב אישור של הארגון להעסיק ספקי משנה או מיקור חוץ.

15.2. התייחסות למיקור חוץ בהתקשרות זאת כספק משנה של הספק.

15.3. כל הנחיות המכרז ונספח אבטחת המידע חלות הן על הספק והן על ספקי המשנה.

15.4. באחריות הספק לוודא כי ספקי המשנה עומדים בכל תנאי ההתקשרות ונספח אבטחת המידע.

15.5. במידה והספק מעסיק ספק משנה המפעיל ומתחזק את מערכות המחשב עבור הספק, הספק יחתים את ספק המשנה על התחייבות כי עליו לעמוד בכל דרישות ההתקשרות. ספק המשנה מחויב בין היתר להעמיד ממונה אבטחת מידע אשר יעמוד בכל הסעיפים בהתקשרות לרבות העברת קורות חיים ואישורו.

15.6. סעיף זה מהווה סעיף יסודי למכרז והפרתו מהווה עילה להפסקת ההתקשרות וחילוט ערבות הספק.

## 16. סיום התקשרות, ניתוק הספק ופרק זמן מותר לשימוש במידע

16.1. במידה ובמהלך תקופת ההתקשרות עולה החשד כי הספק חושף את הב"ה לסיכוני סייבר משמעותיים, בסמכות הב"ה לבצע הפסקת ההתקשרות באופן מידי לפי שיקול דעתה, המלצה לעניין זה תובא לבחינת ועדת המכרזים על ידי הגורם הרלוונטי בארגון.

16.2. הספק מורשה לעשות שימוש במידע על הארגון ומערכותיו רק בתקופת ההתקשרות בלבד ובהתאמה לאופי השירות והתוצרים המסופקים. מותר לספק לשמור מידע שהתקבל מהב"ה או מידע שצבר בזמן העבודה מול הב"ה רק למשך פרק הזמן הנדרש במישרין לביצוע תפקידו לפי החוזה וזאת בצורה מוגנת התואמת את רגישות המידע והסיכונים הרלוונטיים.

16.3. עם סיום ההתקשרות עם הב"ה או בהתאם להחלטה על ניתוק או כאשר הארגון מעוניין להתנתק מהספק במהלך תקופת ההתקשרות או בכל נקודת זמן לפני כן לפי שיקול הב"ה (למשל כשמתרחש אירוע סייבר) יפעל הספק לבצע לאלתר את הפעולות הבאות:

16.3.1. יאפשר להב"ה לנייד את המידע בצורה ישימה וללא צורך בהשקעת משאבים משמעותיים, אך לא לפני שיאפשר להב"ה להעתיק או לנייד את המידע.

16.3.2. יוודא כי כל המידע שהגיע אליו נמחק מכל אמצעי המדיה שברשותו, לרבות כוננים קשיחים, אמצעי גיבוי וכל מדיה מגנטית או אופטית אחר.

16.3.3. יחזיר את כלל הרשומות, הציוד והרכיבים השייכים לארגון אשר נעשה בהם שימוש לצורך עבודת הספק. כל זאת, לרבות פריטים הנמצאים בקרב כלל עובדי הספק וספקי המשנה שלו.

16.3.4. יחתום על הצהרה בה הוא מתחייב שלא נשארו ברשותו רכיבים כלשהם הנוגעים למערכת או מידע אודות הב"ה וכי וידא מחיקת עותקים של קבצים ומידע של המשרד ממערכות המידע (כגון: במחשבים של הספק במקרה שמדובר במחשבים של הספק ששימשו לעיבוד ו/אחסון של מידע של הב"ה).

16.3.5. יחזיר אמצעי הזדהות וגישה פיזית או לוגית למתקנים או למידע של הב"ה (לרבות של עובדי הספק וספקי המשנה שלו).

16.3.6. ינתק את הקישורים למערכות הארגון.

16.3.7. יצהיר כי הוא מוותר על זכותו לתבוע כל זכות קניינית מהב"ה, ובכלל זה את הזכות לקניין רוחני.

16.4. הספק נדרש להיות מחויב לכל הנוגע למותר והאסור אודות פרסום פרטי ההתקשרות לגורמי צד ג'.

16.5. ככל שקיימת הוראה בדין המחייבת שמירת מידע אצל הספק, יש לוודא כי אמצעי האבטחה והבקרה שהוגדרו בחוזה עם הב"ה יישארו אפקטיביים לכל אורך תקופת השמירה.

16.6. ככל שנדרשת על ידי הספק זכות גישה למידע לאחר סיום ההתקשרות לצורך התגוננות בפני תביעות בקשר עם תפקידיו לפי החוזה, ניתן לשמור עותק של המידע באמצעי גיבוי מקובל אצל צד ג' נאמן אשר יהיה רשאי להתיר את הגישה למידע רק למטרות הנ"ל.

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

16.8. בתוך 30 יום מיום בקשת מזמין או תוך 90 יום מסיום ההתקשרות, מכל סיבה שהיא, יעביר הספק למזמין את כל המידע של המזמין, למעט אם המזמין הודיע שהוא אינו מעוניין במידע. ככל שהשירות מאפשר למזמין לאחזר מידע או למחקו ישירות, יאפשר הספק למזמין לבצע זאת עד 30 יום לאחר סיום ההתקשרות, תוך מתן סיוע טכני סביר על ידי הספק לביצוע אחזור המידע או מחיקתו וכן להציג למזמין אסמכתאות כי אכן כלל המידע אוחזר או נמחק בהתאם לנדרש. כלל המידע יאוחזר בפורמט סטנדרטי, עדכני ולא קנייני.

16.9. 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.