שם הגוף: **גלבוע החברה הכלכלית להשקעות ולפיתוח בע"מ** תאריך: _____

נספח א- דרישות אבטחת מידע לספק במיקור חוץ

א. תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 חלות הן על בעל מאגר מידע והן על מחזיק במאגר מידע, כל אחד בהתאם לחובות המוטלות עליו לפי התקנות

ב. אחראי אבטחת המידע רשאי להחמיר או להקל באחד או יותר מהסעיפים הבאים לפי שיקול דעתו, ובהתאם למידע הקיים או מעובד על ידו אצל הספק.

ג. מסמך זה מהווה נספח מחייב להסכם ההתקשרות ומהווה חלק בלתי נפרד מתנאי המכרז.

ד. הוראות נספח זה יחולו על כל ספק, יועץ או נותן שירות אשר במסגרת ההתקשרות עם הארגון מחזיק מידע אישי, מעבד מידע אישי או נחשף למידע אישי של הארגון או של נושאי מידע.

ה. היקף תחולת הדרישות ייקבע בהתאם לאופי השירות, סוגי המידע, היקף הגישה למידע, רמת הסיכון, רמת האבטחה החלה על המאגר, והאם מדובר בשירות טכנולוגי, תפעולי, ייעוצי או אחר

ו. אין בהוראות מסמך זה כדי לגרוע מהוראות חוק הגנת הפרטיות, התשמ"א-1981, לרבות תיקון מס' 13 לחוק, תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, או כל דין אחר החל על הצדדים. במקרה של סתירה בין הוראות מסמך זה לבין הוראות הדין – יחולו הוראות הדין.

ז. דרישות תקנות אבטחת המידע הן כדלקמן:

1. <u>הנחיות כלליות:</u>

1.1. הספק מצהיר ומתחייב כי הוא פועל ויפעל בהתאם להוראות הדין, ובכלל זה חוק הגנת הפרטיות, התשמ"א-1981, התקנות שהותקנו מכוחו, תיקוניו והנחיות הרשות להגנת הפרטיות, וכי הוא נוקט וינקוט אמצעי אבטחה ובקרה הולמים כמתחייב לשם הגנה על המידע האישי המעובד על ידו במסגרת ההתקשרות.

1.2. הספק יעבד מידע אישי רק לפי הוראות בכתב של בעל השליטה במאגר, ורק לצורך ביצוע ההתקשרות, במטרה המוגדרת ובמידה הנדרשת לכך

1.3. הספק ימנה אחראי אבטחת מידע מטעמו, אשר יבטיח שימוש נכון בזיהוי המשתמש ובסיסמא, בהרשאות הגישה למידע ובהגנת משאבי מערכות המחשב והמידע ומערכות התקשורת המכילות מידע השייך לארגון.

1.4. הספק יגדיר נוהל אבטחת מידע, כמפורט בתקנה 4 לתקנות אבטחת המידע. ככל שהוא מחזיק במאגר מידע או מפעיל מערכת מידע עבור הארגון.

1.5. הספק יגדיר מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, הכל בהתאם למפורט בתקנה 5 לתקנות אבטחת המידע, , ככל שהוא מחזיק במאגר מידע או מפעיל מערכת מידע עבור הארגון.

1.6. הספק יבצע סקרי סיכונים, מבדקי חדירה וביקורות תקופתיות, ככל שהדבר חל לפי הדין, לפי רמת האבטחה, מאפייני השירות ודרישת הארגון. ובמקרים בהם הספק מפעיל או מנהל מערכת מידע עבור הארגון. מבלי לגרוע מן האמור, במאגרים שחלה עליהם רמת אבטחה בינונית או גבוהה תיערך ביקורת פנימית או חיצונית לפחות אחת ל-24 חודשים, ובמאגרים שחלה עליהם רמת אבטחה גבוהה יבוצעו גם סקר סיכונים ומבדק חדירה

בתדירות שלא תפחת מהנדרש בדין ובהנחיות הארגון

1.7. הספק מתחייב למסור לארגון, לפי דרישתה, מבדקי אבטחת מידע, סקרי סיכונים, מבדקי חדירה וכל מידע או מסמך אחר הנדרש לצורך בחינת עמידתו בהוראות חוק הגנת הפרטיות, לרבות תיקון מס' 13 לחוק, ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

1.8. החתמת עובדי הספק על הצהרות סודיות הכוללות, בין היתר, התחייבות לשמירה מוחלטת על סודיות המידע של הארגון, שימוש במידע רק בהתאם לאמור בהסכם ההתקשרות בין הספק לארגון ויישום אמצעי האבטחה הקבועים בהסכם ההתקשרות.

1.9. הספק לא יעשה שימוש בספק משנה אשר תהיה לו גישה למידע אישי של הארגון או אשר יעבד מידע אישי של הארגון, אלא לאחר קבלת אישור מראש ובכתב מהארגון. ככל שיינתן אישור כאמור, ייחתם עם ספק המשנה הסכם המחיל עליו חובות זהות לאלו החלות על הספק לפי מסמך זה, והספק יישא באחריות מלאה לפעולותיו ולמחדליו של ספק המשנה.

1.10. התחייבות הספק לא להעביר לצד שלישי מידע שיתקבל במסגרת ההתקשרות, או שימוש במידע שעובדיו יחשפו אליו אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות.

1.11. התחייבות הספק לאפשר לנציג הארגון לערוך ביקורת אבטחה בכל עת.

1.12. הספק ימסור הגדרת איש קשר ייעודי מטעם הספק לכל נושאי אבטחת מידע, גם אם הספק אינו מחויב לכך על פי דין

1.13. חל איסור למסור, להעביר, לעבד או להשתמש במידע לכל מטרה שאינה מוגדרת על ידי הארגון בצורה מפורשת ומתועדת. על ספק השירות, להבהיר את השימושים המותרים לעובדיו, בהתאם להוראות הארגון, תנאי ההתקשרות והוראות הדין.

1.14. הספק לא ייתן הרשאות גישה למידע ללא אישור מראש ובכתב של בעל המאגר או גורם שהוסמך לכך על ידי הארגון.

1.15. הספק יבצע בחינה תקופתית של הרשאות הגישה למערכות המידע ולמאגרי המידע בהם מעובד מידע של הארגון, לצורך וידוא התאמת ההרשאות לתפקיד ולצרכי העבודה בלבד.
הבחינה תכלול בדיקה של בעלי הרשאות פעילים, הרשאות עודפות, משתמשים שאינם פעילים, והרשאות של עובדים שסיימו את תפקידם.
סקר ההרשאות יבוצע לפחות אחת לשנה ,או בתדירות אחרת בהתאם למדיניות אבטחת המידע של הארגון, ויתועד בכתב.
ממצאי הסקר והפעולות שננקטו בעקבותיו יישמרו ויועברו לארגון לפי דרישתה.

1.16. שמירת מידע השבתו ומחיקתו: עם סיום ההתקשרות בין הארגון לבין הספק, מכל סיבה שהיא, או לפי דרישת הארגון, ישיב הספק לארגון, בתוך פרק הזמן שייקבע על ידי הארגון, ובכל מקרה לא יאוחר מ-30 ימים ,אלא אם נקבע מועד קצר יותר בהסכם ההתקשרות, את כלל המידע, הנתונים, הקבצים, המסמכים והתוצרים המצויים בידיו או בידי מי מטעמו במסגרת מתן השירותים.

1.17. סיום התקשרות: ממועד סיום ההתקשרות לא יעשה הספק כל שימוש נוסף במידע, למעט

שימוש הנדרש לצורך השלמת השבת המידע, מחיקתו או שמירתו מכוח דין.

1.17.1. לאחר השבת המידע לארגון, ימחק או ישמיד הספק באופן מאובטח ומלא את כלל עותקי המידע המצויים בידיו או בידי מי מטעמו, לרבות במערכות מידע, סביבות פיתוח ובדיקות, מדיות אחסון, קבצי יצוא, עותקים מודפסים, קבצים זמניים, מטמונים ועותקי גיבוי, כך שלא ניתן יהיה לשחזרם או לעשות בהם שימוש נוסף. לעניין עותקי גיבוי, המחיקה תבוצע בהתאם למחזורי הגיבוי הסבירים והמתועדים של הספק, ובלבד שלא יתאפשר כל שימוש נוסף במידע.

1.17.2. הספק יעביר לארגון אישור חתום בכתב על ביצוע השבת המידע ומחיקתו, לרבות ביחס לספקי משנה, קבלני משנה או כל גורם אחר מטעמו. באישור יפורטו סוגי המידע שנמחקו, מועד המחיקה ואופן המחיקה.

1.17.3. ככל שקיימת חובה לשמור מידע מסוים מעבר לתקופת ההתקשרות מכוח דין, יודיע הספק על כך לארגון מראש ובכתב, יציין את סוג המידע, מקור החובה החוקית ומשך תקופת השמירה. מידע כאמור יישמר בנפרד, בגישה מוגבלת, ולא ייעשה בו כל שימוש למטרה אחרת. בתום תקופת השמירה יימחק המידע והספק יעביר לארגון אישור מחיקה.

1.17.4. הספק לא ישמור מידע מעבר לנדרש לצורך מתן השירותים, ביצוע חובה לפי דין או בהתאם להנחיות הארגון, ויפעל לצמצום מידע עודף גם במהלך תקופת ההתקשרות.

1.17.5. הוראות סעיף זה יחולו גם על ספקי משנה או כל גורם אחר הפועל מטעם הספק במסגרת ההתקשרות.

1.17.6. אי עמידה בהוראות סעיף זה תיחשב כהפרה יסודית של ההתקשרות

1.18. עיבוד מידע מחוץ לישראל: הספק יציין בפני הארגון את מיקום אחסון המידע ואת מיקום עיבוד המידע במסגרת השירותים הניתנים לארגון, לרבות האם המידע נשמר או מעובד בענן, וכן את המדינה או המדינות בהן מצויים שרתי האחסון או מתבצע העיבוד.

1.18.1. לא יועבר מידע אישי מחוץ לישראל ולא יעובד מידע מחוץ לישראל אלא לאחר קבלת אישור מראש ובכתב מבעל המאגר, ובהתאם להוראות חוק הגנת הפרטיות(העברת מידע לחו"ל) והתקנות מכוחו, לרבות הוראות לעניין העברת מידע מחוץ לגבולות המדינה.

1.18.2. ככל שהשירות כולל אחסון או עיבוד מידע בענן או מחוץ לישראל, הספק יתחייב לנקוט באמצעי אבטחת מידע מתאימים התואמים את רמת רגישות המידע ואת הוראות הדין, ובכלל זה הצפנת מידע בתעבורה ובמנוחה, ניהול הרשאות גישה, הפרדה בין לקוחות, תיעוד לוגים, ובקרה על גישה למידע.

2. <u>ניהול כח אדם:</u>

2.1. הספק ייתן וישנה הרשאות גישה למידע המצוי במאגר המידע רק לאחר נקיטת אמצעים סבירים, המקובלים בהליכי מיון ושיבוץ עובדים.

2.2. הספק יקיים הדרכות לבעלי הרשאות גישה למידע המצוי במאגר המידע, בטרם מתן ההרשאות או בטרם שינוי ההרשאות הקיימות. ההדרכות יעסקו בחובות לפי חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "החוק") ותקנות אבטחת המידע ומסירת מידע אודות חובות בעלי ההרשאות לפי החוק ולפי נוהל האבטחה של הספק. ההדרכה תיערך לכל

הפחות אחת לשנה ובהסמכה של בעל הרשאה לתפקיד חדש, סמוך ככל האפשר למועד הסמכתו.

2.3. באם הספק יעביר השירות ו/או המידע ו/או התשתיות ו/או חלק מהם לצד שלישי , יידע את הארגון בכתב, 30 יום לאחר השלמת התהליך באם מדובר בשירות רוחבי לכלל לקוחות הספק, ובמקרה בו מדובר בשירות ייעודי לארגון, יבקש אישורה מראש. אין באמור בסעיף זה כדי לגרוע מן החובה לקבל אישור מראש ובכתב מהארגון בכל מקרה שבו צד שלישי, ספק משנה או גורם אחר מטעם הספק יהיה בעל גישה למידע אישי של הארגון או יעבד מידע אישי עבורו

3. <u>אירועי אבטחת מידע:</u>

3.1. ספק ידווח ללא דיחוי לבעל המאגר (הארגון) על כל אירוע אבטחת מידע הנוגע למידע שבמאגר. במקרה של אירוע אבטחת מידע חמור, בעל המאגר יבחן את חובת הדיווח לרשות להגנת הפרטיות בהתאם להוראות הדין. הספק ישמור תיעוד של אירועי אבטחת המידע באופן מאובטח למשך 24 חודשים לפחות.

3.2. קביעת הוראות בנוהל האבטחה של הספק לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים הנדרשים וכן הוראות לעניין דיווח למנמ"ר/אחראי מחשוב הארגון ולמנהל אבטחת המידע על אירועי אבטחה ועל הפעולות שננקטו בעקבותיהם.

3.3. הספק יבטיח זמינות של גורם מקצועי לטיפול באירועי אבטחת מידע וסייבר.

3.4. הספק יקיים דיון באירועי האבטחה ויבחן את הצורך בעדכון נוהל האבטחה שלו, במאגרים שחלה עליהם רמת אבטחה בינונית, אחת לשנה לפחות. במאגרים שחלה עליהם רמת אבטחה גבוהה, אחת לרבעון לפחות.

3.5. הספק אחראי לחייב להחתים את כל ספקי המשנה שלו הנוגעים לביצוע ההתקשרות לעמוד בתנאיה.

בכבוד רב,
שם מלא_____
דואל:_____
טלפון:_____
חתימה וחותמת:_____

אנו מאשרים את הסכמתנו:_____
חתימת וחותמת חברת הספק

נספח ב- דרישות אבטחת מידע למערכות מידע ולתשתיות המופעלות עבור הארגון

1. מסמך זה מהווה נספח מחייב להסכם ההתקשרות וחלק בלתי נפרד מתנאי המכרז.

1.1. אין בהוראות מסמך זה כדי לגרוע מהוראות חוק הגנת הפרטיות, התשמ"א-1981, לרבות תיקון מס' 13 לחוק, תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, או מכל דין אחר החל על הצדדים. במקרה של סתירה בין הוראות מסמך זה לבין הוראות הדין, יחולו הוראות הדין.

1.2. ככל שהמערכת אינה כוללת מידע אישי כהגדרתו בחוק הגנת הפרטיות, יחולו הוראות מסמך זה רק ככל שהן רלוונטיות לאבטחת המערכת, התשתיות וסביבת ההפעלה

1.3. היקף תחולת הדרישות ייקבע בהתאם לאופי השירות, סוגי המידע, היקף הגישה למידע, רמת הסיכון, רמת האבטחה החלה על המאגר, והאם מדובר בשירות טכנולוגי, תפעולי, ייעוצי או אחר

1.4. הספק ימסור לארגון, לפי דרישה, כל מידע או מסמך הנדרש לצורך בחינת עמידתו בדרישות אבטחת המידע החלות על השירותים, המערכת והתשתיות.

2. דרישות אבטחת המידע החלות על המערכת, התשתיות וסביבת ההפעלה הן כדלקמן

2.1. ספק השירות יבצע את תכנית הגנה על המידע בכל המערכות, על פי תכנית ההגנה על המידע, אשר תקבע על ידי ארגון ו/או בשיתוף עמה. ספק השירות מתחייב ליישם את תכנית ההגנה על המידע, בכל מקרה, אחת לתקופה, כפי שיידרש על ידי ארגון, תיבחן מחדש תכנית ההגנה על המידע ותעודכן בהתאם לצורך. התוכנית כוללת את הסעיפים הבאים אך אינה מוגבלת להם:

2.2. תיעוד ארכיטקטורת המערכת

ככל שהמערכת מנוהלת בחצרי הספק או במודל ענן, יעביר הספק למנהל אבטחת המידע של הארגון תרשים רשת מעודכן של סביבת העבודה, הכולל את תחנות הקצה, רכיבי הרשת, רכיבי אבטחת המידע ומערכות האחסון המשמשות את המערכת. התרשים יכלול גם פירוט של היצרנים ומערכות ההפעלה בשימוש. הספק יעדכן את התרשים אחת לשנה לפחות או בכל שינוי מהותי בתשתית.

2.3. מדיניות אבטחת מידע

הספק יעביר לארגון מסמך מדיניות אבטחת מידע המפרט את מנגנוני הבקרה ואופן ניהול הגישה וההגנה למערכותיו. הארגון יהיה רשאי להעביר הערות והנחיות לתיקון, והעברת מידע למערכת תתבצע רק לאחר אישור הארגון למסמך זה.

2.4. עדכוני אבטחה וניהול פגיעויות

על הספק לוודא התקנה שוטפת של עדכוני אבטחה קריטיים לכל מערכות המחשוב שבאחריותו. לא יעשה שימוש בציוד, תוכנה או חומרה שאינם נתמכים על ידי היצרן, אלא אם הועברה לארגון תכנית מתוחמת בזמן לשדרוג המערכות.

2.5. אבטחת מחשבים ניידים

במחשבים ניידים מהם ניתן לגשת לנתוני המערכת תוגדר הצפנה מלאה של הדיסק.

המשתמשים יונחו שלא לשמור מידע מהמאגר על המחשב המקומי. כל גישה לנתוני המאגר תחייב הזדהות הכוללת לפחות שני אמצעי זיהוי.

2.6. הצפנת מידע בתעבורה

כל הנתונים המועברים בין מערכות המחשוב יוצפנו טרם העברתם בתווך התקשורת. ההצפנה תבוצע באמצעים המאושרים על ידי הארגון ותוחל הן ברשתות חוטיות והן ברשתות אל-חוטיות.

2.7. זמינות למענה באירוע אבטחה

ספק השירות יקצה לפחות שני אנשי קשר בעלי הרשאות מתאימות לטיפול באירועי אבטחת מידע, וימסור את פרטי ההתקשרות שלהם למנהל אבטחת המידע של הארגון

2.8. תיעוד בלוג:

2.8.1. חותמת זמן ברמת שניות

2.8.2. מזהה משתמש (כגון IP, UID)

2.8.3. נסיונות גישה

2.8.4. נעילות משתמש

2.8.5. פעולות עדכון ע"י המשתמשים, כולל שמירת ערך קודם.

2.8.6. העלאות תכנים

2.8.7. ייצור והורדת קובץ

2.8.8. גישה מרחוק

2.8.9. שינויים במערך ההרשאות

2.8.10. אירועי אבטחת מידע

2.8.11. שמירת הלוגים הנ"ל באופן מאובטח, למשך 24 חודשים, לכל הפחות.

2.8.12. קיום נוהל בדיקה שגרתי של הלוגים למנגנון הבקרה כולל דו"ח של הבעיות שהתגלו והצעדים שננקטו בעקבותיהן.

2.8.13. תיעוד כל מקרה שבו התגלה אירוע אבטחת מידע. ככל האפשר יבוסס התיעוד על רישום אוטומטי.

2.8.14. הגישה ללוגים תוגבל לגורמים מורשים בלבד ותבוצע בקרה על הגישה אליהם.

2.8.15. דיווח למנהל אבטחת המידע בארגון במקרה של אירוע אבטחת מידע.

2.9. אבטחה פיזית וסביבתית:

2.9.1. הספק ישמור את מאגרי המידע וכן את התשתיות והמערכות המשמשות את המאגרים, במקום מוגן, המונע חדירה וכניסה אליו ללא הרשאה והתואם את אופי פעילות המאגר ורגישות המידע.

2.9.2. הספק יבצע בקרה ותיעוד של הכניסה והיציאה מאתרים בהם מצויות מערכות המידע וכן בקרה ותיעוד של הכנסה והוצאת ציוד אל מערכות המאגר ומהן.

2.9.3. הספק יערוך ביקורת פנימית או חיצונית, לעניין עמידתו בתקנות אבטחת מידע, אחת לשנתיים לפחות. הביקורת תיערך ע"י גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שאיננו אחראי האבטחה על המאגרים.

2.9.4. הספק יגביל/ ימנע אפשרות חיבור התקנים ניידים וינקוט אמצעי הגנה.

2.9.5. הספק לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, ללא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש.

2.10. גיבויים

2.10.1. בסיס הנתונים יגובה לפחות פעם ביום באופן שיאפשר שחזור מלא בעת הצורך.

2.10.2. ביצוע שחזור רבעוני יזום ודיווח לארגון.

2.10.3. ניסוי DR מלא אחת לשנה.

2.10.4. במאגרים שחלה עליהם רמת אבטחה בינונית או גבוהה, הספק יקבע ויישם נהלים לביצוע גיבוי תקופתי שגרתי ולהבטחת יכולת שחזור הנתונים, בהתאם לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

2.11. אנונימיזציה, השחרה וארכוב מידע

2.11.1. המערכת תאפשר לארגון לבצע פעולות של מחיקה, אנונימיזציה, השחרת שדות או העברת מידע לארכיון, בהתאם למדיניות שמירת המידע של הארגון ולהוראות הדין.

2.11.2. במסגרת זו תאפשר המערכת, בין היתר:

2.11.2.1. אנונימיזציה של מידע אישי באופן שלא יאפשר זיהוי ישיר או עקיף של נושא המידע.

2.11.2.2. השחרת שדות מזהים במידע אישי, כך שלא ניתן יהיה לזהות את האדם אליו מתייחס המידע.

2.11.2.3. העברת רשומות שאינן פעילות או שאינן נדרשות לארגון עוד לצורך מתן השירות לארכיון במערכת.

2.11.2.4. מחיקה או אנונימיזציה של מידע עודף בהתאם להנחיות הארגון ולעקרון צמצום המידע.

2.11.2.5. פעולות כאמור יתועדו במערכת באמצעות מנגנוני לוגים מתאימים, לצורך בקרה ופיקוח.

2.11.2.6. במקרים בהם קיימות תלותיות בין טבלאות או רשומות (Relations / Foreign Keys), ייושמו מנגנונים מתאימים כגון אנונימיזציה, השחרת שדות, מחיקה לוגית או ניתוק הקשר בין הרשומות, כך שלא תיחסם האפשרות למחוק את הרשומה או הטופס הרלוונטי.

2.11.2.7. המערכת תאפשר ביצוע מחיקה מלאה של רשומה או טופס גם אם חלק מהשדות או המידע אינם ניתנים למחיקה מסיבות טכניות, וזאת באמצעות מנגנונים חלופיים כגון אנונימיזציה או השחרה של המידע המזהה.

2.11.3. פיתוח מאובטח:

2.11.3.1. הספק יוכיח שימוש בתקן OWASP או מקביל שיאושר ע"י מנהל אבטחת המידע של הארגון.

2.11.3.2. הספק יוכיח שימוש בגרסאות מעודכנות ונתמכות של שפות הפיתוח.

2.11.3.3. ככל שמתבצע פיתוח או התאמה למערכת,לפני כל פיתוח הספק יעביר מסמך אפיון מערכת לאישור של מנהל אבטחת מידע וסייבר של הארגון.

2.11.3.4. ביצוע בדיקות מסירה ע"י הספק לווידוא קיום דרישות אבטחת מידע באפיון.

2.11.3.5. מבדק חדירה למערכת לפני העברה לייצור.

2.11.3.6. שימוש ברכיבי קוד פתוח ורכיבי צד שלישי

2.11.3.7. הספק יפרט, לפי דרישת הארגון, האם המערכת עושה שימוש ברכיבי קוד פתוח או ברכיבי צד שלישי מהותיים, ויהיה אחראי לתחזוקתם, לעדכוני אבטחה שוטפים, לטיפול בחולשות ידועות ולעמידה בתנאי הרישוי החלים עליהם.

2.11.3.8. השימוש ברכיבים כאמור לא יפגע בזכויות הארגון במערכת ולא יחייב חשיפת מידע של הארגון או של קוד שפותח עבורה, אלא אם נדרש אחרת במפורש לפי דין או לפי תנאי ההתקשרות.

2.12. קוד מקור

2.12.1. לא יבוצעו עבודות פיתוח על מערכת הייצור (Production) אלא על מערכות ייעודיות לצורך הפיתוח (להלן סביבת פיתוח). סביבת הפיתוח תהיה נפרדת ממערכת הייצור. רק לאחר סיום הבדיקות בסביבת הפיתוח, יהיה שינוי גרסה במערכת הייצור כל עדכון של מערכת הייצור מחייב תיאום ואישור של הארגון ו לאחר ווידא להעדר קוד זדוני ובדיקת הקוד לאבטחת מידע.

2.12.2. בכל מקרה של כתיבת קוד על ידי הספק, על הספק לעמוד בדרישות של פיתוח מאובטח.

2.12.3. ככלל, שימוש בנתונים ממערכת האמת לצורך פיתוח, יבוצע לאחר שינויי נתוני האמת (Scrambling) כך שלא ניתן יהיה לזהות או להצליב את הנתונים עם זיהוי אדם בנותני מערכת הפיתוח. חריגה מכלל זה, תחייב אישור של מנהל אבטחת המידע של הארגון.

2.12.4. הספק יתקין תוכנת הגנה תקנית, מסחרית ומעודכנת נגד נוזקות על כל מחשב ושרת המשמש לתפעול המערכת או המכיל מידע השייך לארגון

2.12.5. ככל שהדבר רלוונטי ובהתאם לתנאי המכרז, ייבחן מנגנון הפקדת קוד מקור אצל נאמן

2.12.6. הספק יבצע בדיקות אבטחת קוד (Code Review / SAST) לפי סטנדרטים מקובלים

2.12.7. הספק יבצע הדרכה פרונטלית על התוכנה עפ״י דרישת הארגון.

2.12.8. המערכת תהיה מותקנת על שרתי הארגון או מבוססת ענן או בחצרי הספק.

2.12.9. ככל שנדרש ממשק למערכות ארגוניות, המערכת תאפשר API מאובטח המאפשר ממשק למערכות ליבה פנים ארגוניות, דוגמת CRM, ERP וכד׳.

2.13. הגנה אפליקטיבית:

2.13.1. שימוש בפרוטוקול Https בכל דפי היישום אם המערכת בענן או על גבי האינטרנט.

2.13.2. באם מדובר במערכת עם ממשק WEB, מניעת אפשרות למניפולציה של כתובת ה-URL (חוסר יכולת לשנות UID בסוף הדף, לא ניתן לשנות או להוסיף דפי משנה).

2.13.3. הגדרת רשימת ערכים וטווחים מותרים לשדות קלט, תוך עדיפות לרשימה סגורה של ערכים (כולל הגנה על FORM באמצעות CAPTCHA).

2.13.4. וידוא שאין בדו״חות המופקים מהמערכת חשיפה של שדות שלא נדרשים.

2.13.5. אין לחשוף למשתמש הקצה הודעות שגיאה אפליקטיביות העלולות להסגיר קוד וטבלאות בתוך היישום. שגיאות כאלה יש לכתוב לקובץ לוג בלבד או לתת הודעה גנרית.

2.13.6. במקרה של העלאת קבצים למערכת: יש לוודא כי קובץ העולה לשרת יעבור סניטציה ויישמר בשרת כקובץ בעל סיומת לא פוגענית הקובץ יישמר ללא יכולת הרצה (כגון שינוי סיומת / אחסון מחוץ לשרת האפליקציה).

2.13.7. הפרדה, ככל הניתן, בין המערכות אשר ניתן לגשת מהן למידע שבמאגר, לבין מערכות מחשוב אחרות שמשמשות את הספק.

2.13.8. שימוש במערכות הפעלה, דפדפנים, בסיסי נתונים ותשתיות תוכנה בגרסאות נתמכות בלבד.

2.13.9. במידה ויש צורך בגישה למערכת מחוץ לסביבה הארגונית או ממכשיר סלולרי, יש להקפיד על אמצעי הגנה ושימוש בשיטות הצפנה מקובלות להגנה על המידע (זיהוי אישי, הצפנת תווך הגישה, ניטור פעולות בגישה מרחוק, חוק FW ייעודי עבור ספק המבצע תחזוקה במערכת).

2.14. בקרת גישה:

2.14.1. הגדרת אימות כפול בכניסה למערכת- בעת הקשת משתמש וסיסמה

2.14.2. הגדרת Session Time Out לאחר פרק זמן של אי פעילות, המחייב זיהוי מחדש של המשתמש.

2.14.3. פרק הזמן לסיום Session יוגדר בהתאם למדיניות אבטחת המידע של הארגון ולא יעלה על 30 דקות, ככל שהדבר ניתן מבחינה טכנולוגית.

2.14.4. נקיטת אמצעי אבטחה הולמים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת או אל קווי התקשורת בין הארגון אל הספק (לכל הפחות Firewall- ו-IPS, הצפנת TLS1.2).

2.15. גישה מרחוק

כל גישה למערכת מחוץ לרשת הארגון תבוצע בצורה מוצפנת ותכלול הזדהות באמצעות שני אמצעי זיהוי לפחות. גישה מרחוק תתאפשר רק לאחר אישור מפורש של מנהל המאגר או גורם שהוסמך לכך ושל מנהל אבטחת המידע של הארגון.

2.16. הזדהות והרשאות:

2.16.1. מתן הרשאות גישה למאגרי המידע ולמערכות המאגרים, בהתאם להגדרות התפקיד ובמידה הנדרשת לביצוע התפקיד בלבד ומידור גישה/ עדכון ברמת שדה.

2.16.2. רישום מעודכן של תפקידים, הרשאות הגישה שניתנו ובעלי ההרשאות הממלאים תפקידים אלה ויכולת הפקה יזומה של דו"ח הרשאות תקפות אחת לשנה לפחות, או עפ"י דרישת הארגון.

2.16.3. יישום תיעוד לכל שינוי בטבלת ההרשאות.

2.16.4. ככל הניתן, אופן הזיהוי ייעשה על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.

2.16.5. אופן הזיהוי של משתמש ניהול (Admin) יכלול שם משתמש וסיסמא, וישלב מזהה נוסף - OTP, כתובת IP קבועה, או שדה אחר.

2.17. שימוש במדיניות סיסמאות:

2.17.1. אורך סיסמא מינימלי - 8-10 תווים.

2.17.2. מורכבות סיסמא - שימוש באותיות וספרות.

2.17.3. ניתן להשתמש ב-OTP.

2.17.4. ניתן לקשר ל-AD.

2.17.5. אכיפת החלפת סיסמא ראשונית.

2.17.6. שימוש בקאפצ'ה לאחר 2 נסיונות גישה שגויים.

2.17.7. חסימת משתמש לאחר 5 ניסיונות גישה שגויים.

2.17.8. חסימת משתמש שלא הזדהה 180 ימים.

2.17.9. הסיסמאות תוחלפנה כל 180 ימים לפחות.

2.17.10. הצפנת הסיסמאות בהצפנה חד כיוונית בבסיס הנתונים.

2.17.11. מניעת השלמה אוטומטית של הסיסמא.

2.17.12. אימות דו שלבי בכניסה למערכת

2.17.13. הגדרת אופן טיפול בתקלות הקשורות באימות זהות.

2.17.14. ביטול הרשאות לבעל הרשאה שסיים את תפקידו ובמידת האפשר שינוי סיסמאות למאגר ולמערכות המאגר, שבעל ההרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל ההרשאה.

2.18. דרישות במקרה של פעילות בענן:

2.18.1. שימוש ב-WEB SERVICE או STORED PROCEDURES על מנת למנוע ממשק ישיר בין המשתמש לשרת בסיס הנתונים.

2.18.2. שימוש בגרסאות דפדפנים נתמכות.

2.18.3. ממשק ניהול בגישה מהארגון בלבד או מכתובות שיסופקו על ידה.

2.18.4. במקרה של ניהול בענן, ייושמו אמצעי הגנה מתאימים בהתאם לארכיטקטורה ולרמת הסיכון, כגון WAF, IDS/IPS, שירותי ניטור והגנה מנוהלים, לפי דרישת הארגון.

2.18.5. מימוש הצפנה בתקשורת באמצעות פרוטוקול TLS 1.2 או פרוטוקול אחר שיאושר ע"י מנהל אבטחת המידע בארגון.

2.18.6. הספק יבטיח הפרדה לוגית בין נתוני הארגון לבין נתוני לקוחות אחרים.

2.19. אבטחת תשתיות:

2.19.1. הפרדת סביבות:

2.19.1.1. סביבת הייצור תופרד מסביבות אחרות.

2.19.1.2. העברת אפליקציה מסביבת פיתוח לייצור תתבצע בצורה מבוקרת.

2.19.1.3. לא יעשה שימוש בנתונים אמיתיים בסביבת הפיתוח, אלא במקרים חריגים באישור הארגון.

2.19.2. ביצוע עדכוני אבטחה שוטפים למערכות. עדכוני אבטחת מידע CRITICAL בשרתים ברמה רבעונית.

2.19.3. בסיס נתונים ייעודי לארגון - הספק יבצע הפרדה בין בסיס הנתונים של הארגון לבין בסיסי נתונים של לקוחות אחרים.

2.19.4. הגנת בסיס הנתונים והקשחתו עפ"י הנחיות הארגון.

2.19.5. ניטור שינויים בבסיסי הנתונים והפקת דו"ח לארגון לפי דרישתה.

2.19.6. זמינות מרבית – יידוע על כל השבתה של המערכת.

2.19.7. הספק ישמור את המידע במערכת כל עוד נדרש לצורך מתן השירות, בהתאם להוראות בעל המאגר, למדיניות שמירת המידע של הארגון ולהוראות כל דין.

2.19.8. הספק יספק לארגון יכולת שליטה ובקרה על הנתונים בענן וכן אפשרות חד צדדית להפסקת השימוש בשירותי הענן תוך מחיקת המידע באופן שלא ניתן לאחזור.

אני החתום מטה, מתחייב לבצע את המפורט בהצהרה זו, בשם הספק, חב' _____.

_____	_____	_____
תאריך	שם מורשה החתימה	חותמת וחתימה

נספח ג-הצהרת על עמידה בדרישות חוק הגנת הפרטיות ותיקון 13

תאריך: _____/_____/____

<u>הנדון: הצהרה על עמידה בדרישות הגנת הפרטיות בהתאם</u>

<u>לתיקון 13 לחוק הגנת הפרטיות (להלן החוק)</u>

פרשנות:

בעל השליטה במאגר מידע	_____ , וגופי הסמך מטעמה
הספק/היועץ הזוכה	הזוכה בהליך התקשרות עם בעל המאגר

בהתאם לחוק הגנת הפרטיות ובפרט תיקון 13 לחוק הגנת הפרטיות, התשפ"ד-2024, שנכנס לתוקף ביום 14.8.2025, חלים חובות ואחריות על בעל המאגר, על המחזיק בו ועל המשתמשים בו, כל אחד לפי מעמדו והוראות הדין, לרבות חובות גילוי, בקרה ופיקוח על יישום הדרישות.

הצהרה זו אינה באה אלא להוסיף על הדרישות המפורטות בדין, ובכל מקרה של סתירה או פרשנות הוראות הדין גוברות על הצהרה זו.

הספק הזוכה, ימלא בקפדנות את הדרישות המפורטות בתקנות וכן את הנחיות בעל השליטה במאגר ו/או מי מטעם בעל המאגר הממונה על הגנת הפרטיות ו/או יועץ המשפטי של הארגון, ככל שתתקבל כל דרישה או הנחיה הקשורה לתקנות. הספק הזוכה יבצע את הפעולות הבאות כמחזיקי המאגר / המאגרים השייכים לבעל המאגר וכן כמשתמשים במאגר (לכל מטרה שהיא, אף למטרות תחזוקה שוטפת וגיבוי של הנתונים הקיימים בו).

הספק הזוכה יישם את כלל הדרישות ולבצע את כל הפעולות המפורטות בהצהרה זו - על חשבונו, ללא כל דרישה כספית וללא תשלום נוסף מצד הארגון מעבר לתשלומים המפורטים במחירון המכרז.

ככל שיוטלו עיצומים כספיים, קנסות או חיובים אחרים על בעל המאגר, הנובעים במישרין או בעקיפין מהפרת הוראות הדין, התקנות או הוראות ההתקשרות על ידי הספק הזוכה או מי מטעמו, יישא הספק הזוכה באחריות למחדליו וישפה את בעל המאגר בגין כל נזק, הוצאה או חיוב כספי שייגרמו עקב כך, לרבות הוצאות משפטיות והוצאות נלוות

ככל שהעיצומים או הנזקים נובעים ממחדלים של בעל המאגר או ממחדלים משותפים של בעל המאגר ושל הספק הזוכה, תיקבע חלוקת האחריות והנשיאה בהוצאות בין הצדדים בהתאם לחלקו היחסי של כל צד במחדל, וזאת בהסכמה בין הצדדים, ובהיעדר הסכמה – בהתאם למנגנון יישוב המחלוקות הקבוע בהסכם ההתקשרות

הגדרות:

בעל המאגר / בעל השליטה במאגר - הארגון, אשר קובע את מטרות העיבוד של המידע האישי ואת אופן השימוש בו במסגרת פעילותה.
מאגר מידע- אוסף של נתונים המוחזק באמצעי ממוחשב ומאורגן באופן המאפשר איתור ושליפה של מידע לפי אדם מסוים או לפי מאפיינים מזהים אחרים, כהגדרתו בחוק הגנת הפרטיות, התשמ״א-1981.
הספק/היועץ - הזוכה במכרז זה או כל גורם מטעמו המספק ומבצע פעולת עיבוד לארגון.
מחזיק במאגר מידע - מי שמחזיק מידע אישי או מעבד אותו עבור בעל המאגר במסגרת מתן השירותים.
מידע אישי - כל נתון המתייחס לאדם מזוהה או לאדם שניתן לזהותו, במישרין או בעקיפין, לרבות פרטי זיהוי, פרטי קשר, מידע כלכלי, רפואי או כל מידע אחר הנוגע לאדם מידע כהגדרתו בחוק הגנת הפרטיות, התשמ״א-1981.
עיבוד מידע - כל פעולה או סדרת פעולות המתבצעות במידע אישי, לרבות איסוף, קליטה, רישום, אחסון, עיון, שימוש, העברה, התאמה, שינוי, מחיקה או השמדה של מידע.
נושא מידע אדם אשר המידע האישי מתייחס אליו.

1. **תחולת הנספח** :הוראות נספח זה יחולו על כל ספק, יועץ, נותן שירות או גורם חיצוני אשר במסגרת ההתקשרות עם הארגון מחזיק מידע אישי, מעבד מידע אישי או נחשף למידע אישי של הארגון או של נושאי מידע. הספק מתחייב לפעול בהתאם להוראות חוק הגנת הפרטיות, התשמ״א-1981, התקנות מכוחו, הנחיות הרשות להגנת הפרטיות והוראות תיקון 13 לחוק. אין בהוראות נספח זה כדי לגרוע מהוראות הדין, ובכל מקרה של סתירה בין הוראות מסמך זה לבין הוראות הדין – יחולו הוראות הדין.
2. **מעמד הספק ביחס למידע**: ככל שהספק מחזיק במידע אישי או מעבד אותו עבור הארגון, ייחשב הספק כמחזיק במאגר מידע בהתאם להוראות חוק הגנת הפרטיות. סוגי המידע המעובד, מטרות העיבוד וקטגוריות נושאי המידע נקבעים על ידי בעל המאגר בלבד. הספק

אינו רשאי לעשות כל שימוש עצמאי במידע אישי ואינו רשאי לקבוע מטרות עיבוד או לעשות שימוש במידע מעבר לנדרש לצורך מתן השירותים לארגון

3. **מטרות עיבוד מידע אישי**: הספק יעבד מידע אישי אך ורק בהתאם להוראות בכתב של בעל המאגר ולצורך מתן השירותים במסגרת ההתקשרות בלבד. הספק לא יעשה כל שימוש נוסף במידע אישי, לרבות שימוש מסחרי, מחקרי, סטטיסטי, שיווקי, פיתוח מוצרים, ניתוח נתונים, אימון מערכות בינה מלאכותית או כל שימוש משני אחר, אלא אם ניתן לכך אישור מפורש מראש ובכתב מבעל המאגר.
4. **עקרון צמצום המידע**: הספק מתחייב לעבד מידע אישי רק במידה הנדרשת לצורך מתן השירותים ולהימנע מאיסוף, שמירה או שימוש במידע עודף שאינו נדרש לצורך ביצוע ההתקשרות
5. **ממונה הגנת פרטיות**: ככל שיידרש על פי דין, ימנה הספק הזוכה ממונה על הגנת הפרטיות (DPO) מטעמו, לצורך עמידה בהוראות הדין והתקנות בתחום הגנת הפרטיות ואבטח המידע.

הממונה על הגנת הפרטיות של המזמין יהיה אחראי על הפיקוח הכולל ליישום דרישות החוק, על ביצוע בקרות ובדיקות שוטפות במאגרי המידע של המזמין, ועל העברת הנחיות מקצועיות הן לספק הזוכה והן לגורמים הרלוונטיים במזמין, בהתאם לתפקידו ולחובותיו לפי דין.

6. **סודיות ושמירת מידע**: הספק מתחייב לשמור בסודיות מלאה כל מידע אישי שיגיע לידיו במסגרת ההתקשרות ולא להעבירו לצד שלישי אלא אם הדבר נדרש לצורך מתן השירותים ובהתאם להוראות בעל המאגר והוראות הדין. הספק יוודא כי עובדיו וכל גורם מטעמו שיש לו גישה למידע אישי יהיו כפופים להתחייבות לשמירת סודיות.
7. **שימוש בספקי משנה**: הספק לא יעביר עיבוד מידע אישי לספק משנה או לגורם אחר אלא לאחר קבלת אישור מראש ובכתב מבעל המאגר. ככל שאושר שימוש בספק משנה, יחולו על ספק המשנה כל ההתחייבויות החלות על הספק לפי נספח זה, והספק יהיה אחראי לפעולותיו של ספק המשנה כאילו היו פעולותיו שלו.
8. **הפרדת מידע ובעלות במידע**: הספק יבטיח כי מידע אישי של הארגון יישמר בנפרד ממידע של לקוחות אחרים של הספק, ולא יעשה שימוש במידע של הארגון לצורך יצירת מאגר מידע עצמאי או לכל מטרה שאינה מתן השירותים לארגון. כל מידע אישי המועבר לספק במסגרת ההתקשרות הינו קניינו של בעל המאגר בלבד, והספק לא ירכוש כל זכות במידע.
9. **סיוע במימוש זכויות נושאי מידע**: הספק יסייע לבעל המאגר, לפי דרישתו וללא דיחוי, במימוש זכויות נושאי המידע בהתאם להוראות חוק הגנת הפרטיות, לרבות זכות העיון במידע אישי, תיקון מידע או מחיקתו.
10. **השבת מידע ומחיקתו בסיום התקשרות**: עם סיום ההתקשרות בין הצדדים, מכל סיבה שהיא, ישיב הספק לבעל המאגר את כלל המידע האישי שהועבר לידיו במסגרת ההתקשרות. לאחר השבת המידע ימחק הספק כל עותק של המידע המצוי בידיו או בידי מי מטעמו, לרבות עותקי גיבוי ומדיות אחסון, ויעביר לבעל המאגר אישור מחיקה בכתב, בכפוף להוראות הדין.
11. **דיווח על פגיעה בפרטיות**: הספק יודיע לבעל המאגר ללא דיחוי על כל חשש לפגיעה בפרטיות או שימוש בלתי מורשה במידע אישי שהגיע לידיעתו במסגרת מתן השירותים.
12. **אחריות לעיצומים ונזקים**: ככל שיוטלו על בעל המאגר עיצומים כספיים, קנסות או חיובים אחרים הנובעים מהפרת הוראות חוק הגנת הפרטיות או הוראות ההתקשרות על ידי הספק

או מי מטעמו, יישא הספק באחריות למחדליו וישפה את בעל המאגר בגין הנזקים וההוצאות שנגרמו עקב כך.

13. **פיקוח ובקרה**: בעל המאגר יהיה רשאי לדרוש מהספק מידע או מסמכים הנדרשים לצורך בחינת עמידתו בהוראות חוק הגנת הפרטיות ובהוראות נספח זה, והספק מתחייב לפעול בהתאם להנחיות הממונה על הגנת הפרטיות מטעם הארגון בכל הנוגע לעיבוד מידע אישי במסגרת ההתקשרות.

אני החתום מטה, מתחייב לבצע את המפורט בהצהרה זו, בשם הספק, חב' _____.

_____	_____	_____
תאריך	שם מורשה החתימה	חותמת וחתימה