נספח ח'

<u>כתב התחייבות- הגנת פרטיות</u>

התחייבות זו מהווה חלק בלתי נפרד מהסכם מס' 34/18 למתן שירותי תיאום פיקוח ובקרה לניסוי "נעים לירוק 3" ("**ההסכם**") בין חברת נתיבי איילון בע"מ (כהגדרתה בהסכם – "**החברה**") לבין _____ (כהגדרתו בהסכם – "**נותן השירותים**") ביום _____ אשר תנאיו חלים על יחסי הצדדים יחד עם תנאי התחייבות זו.

במסגרת ההתקשרות בין הצדדים, יספק נותן השירותים לחברה שירותי ניהול, תיאום, פיקוח ובקרה של ניסוי נעים לירוק, המפורטים בהסכם ובמפרט הטכני המצורף כחלק ממסמכי המכרז להסכם כנספח א' (כהגדרתם בהסכם – "**השירותים**"). כחלק ממתן השירותים תהיה לנותן השירותים גישה למידע אישי אודות המתנדבים (כהגדרתם בהסכם) לרבות נתונים אישיים של המתנדבים, המידע המתקבל ממכשירי הניטור המותקנים ברכבם, תוצאות הניסוי ונתוני ההתחשבנות עם המתנדבים וכל מידע נוסף הנוגע למתנדבים ("**המידע**") אשר יישמר במאגר מידע שיוחזק על-ידי נותן השירותים (כהגדרתו בהסכם – "**מאגר המידע**"). לכן מתחייב נותן השירותים כדלקמן:

1. **<u>מטרת השימוש במידע</u>. שימוש במידע ייעשה אך ורק בהתאם למטרה הכלולה בטופס ההודעה וההסכמה ("המטרה") עליו חתמו המתנדבים כתנאי לשימוש במידע והמצורף בזאת כמוסף א'1. לא תתבצע שום פניה לקבלת מידע מהמתנדבים על-ידי נותן השירותים. נותן השירותים מתחייב לעשות שימוש במידע אך ורק לצורך המטרה.**

2. **<u>מתן זכות עיון ותיקון</u>. נותן השירותים יעמוד בדרישות סעיפים 13 -14 לחוק הגנת הפרטיות, תשמ"א-1981 ("החוק"), ויאפשר למתנדבים, לבאי כוחם או לאפוטרופוס שלהם לעיין במידע אודותם תוך 7 ימים מקבלת בקשת העיון, ולבקש לתקן או למחוק מידע זה ויעדכן את המתנדבים אודות זכויותיהם ודרכי מימושם.**

3. **<u>אבטחת מידע</u>. נותן השירותים יעמוד בדרישות תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 ("תקנות האבטחה"), החלות על מאגרי מידע בעלי רמת אבטחה גבוהה כהגדרתם בתקנות האבטחה, לרבות ומבלי לגרוע:**

3.1. <u>ממונה על אבטחה</u>. נותן השירותים ימנה ממונה על אבטחת מידע ("**הממונה**") בהתאם לסעיף 17ב לחוק וסעיף 3 לתקנות האבטחה. הממונה יהיה כפוף ישירות למנהל מאגר המידע ויהיה אחראי, בין היתר, על הכנת נוהל האבטחה (כמפורט בסעיף 3.2 להלן) ותכנית לבקרה שוטפת על עמידת נותן השירותים בדרישות תקנות האבטחה. נותן השירותים יקצה לממונה את המשאבים הדרושים לשם מילוי תפקידו.

3.2. <u>נוהל אבטחה</u>. נותן השירותים ינסח נוהל אבטחה בהתאם למסמך הגדרות מאגר המידע, ובהתאם לראשי הפרקים המצורפים להתחייבות זו כמוסף א' לנספח זה ותקנות האבטחה לרבות סעיפים 2 ו-4 לתקנות האבטחה. נותן השירותים ישמור את נוהל האבטחה כך שפרטים ממנו יימסרו לגורמים המורשים (כהגדרתם בסעיף 4.2 להלן) רק בהיקף נדרש לצורך ביצוע תפקידם. אחת לשנה, נותן השירותים יבחן את הצורך בעדכון נוהל האבטחה, אלא אם כן: א) נעשו שינויים מהותיים במערכות מאגר המידע או בתהליכי עיבוד המידע; או ב) נודע לנותן השירותים על

סיכונים טכנולוגיים חדשים הנוגעים למערכות מאגר המידע. במקרים אלה נותן השירותים יבחן באופן מיידי את הצורך בעדכון נוהל האבטחה.

3.3. מסמך מבנה מאגר המידע ורשימת מערכות מאגר המידע. נותן השירותים יחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות מאגר המידע בהתאם לראשי הפרקים המצורפים להתחייבות זו כמוסף ב' לנספח זה תקנות האבטחה לרבות סעיף 5 לתקנות האבטחה. נותן השירותים ימסור את הפרטים הכלולים במסמכים הנ"ל אך ורק לעובדיו המורשים ורק בהיקף הנדרש לצורך ביצוע תפקידיהם.

3.4. סקר סיכונים. נותן השירותים יערוך, אחת ל-18 חודשים, סקר לאיתור סיכוני אבטחת מידע בהתאם לסעיף 5 לתקנות האבטחה, ידון בתוצאות הסקר, יבחן את הצורך בעדכון נוהל האבטחה ויתקן כל ליקוי שיתגלה במסגרת הסקר.

3.5. מבדקי חדירות. נותן השירותים יערוך, אחת ל-18 חודשים, מבדקי חדירות למערכות מאגר המידע לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים, ידון בתוצאות מבדקי החדירות ויתקן כל ליקוי שיתגלה במסגרת מבדקי החדירות ויעמוד בתנאי סעיף 5 לתקנות האבטחה.

3.6. אבטחה פיזית וסביבתית. נותן השירותים ישמור את מערכות מאגר המידע בהתאם לסעיף 6 לתקנות האבטחה. מערכות מאגר המידע יישמרו במקום מוגן המונע חדירה וכניסה אל מאגר המידע בלא הרשאה, והתואם את אופי פעילות מאגר המידע ורגישות המידע. נותן השירותים יבקר ויתעד כל כניסה ויציאה מאתרים שבהם מצויות מערכות מאגר המידע וכל הכנסה והוצאה של ציוד אל מערכות מאגר המידע ומהן.

3.7. אבטחת מידע בניהול כוח אדם. נותן השירותים לא יאפשר גישה למידע ולא ישנה את היקף ההרשאה שניתן לגורם המורשה, אלא רק לאחר שנקט אמצעים סבירים, המותאמים לרגישות המידע ולהיקף הרשאת הגישה שינתן, כדי לוודא שהגורם המורשה מתאים לקבלת גישה למידע, ורק לאחר שקיים הדרכה לגורם המורשה בנושא חובותיו על-פי נוהל האבטחה והחוק. בכל מקרה, אחת לשנתיים יקיים נותן השירותים הדרכות לכלל הגורמים המורשים באשר לחובותיהם על-פי נוהל האבטחה, תקנות האבטחה והחוק, בהיקף הנדרש לצורך ביצוע תפקידיהם, ויעמוד נותן השירותים בתנאי סעיף 7 לתקנות האבטחה.

3.8. ניהול הרשאות גישה. נותן השירותים יקבע הרשאות גישה למידע ולמערכות מאגר המידע, בהתאם לתנאי סעיף 8 לתקנות האבטחה, להגדרות תפקיד ובמידה הנדרשת לביצוע התפקיד בלבד וינהל רשימה מעודכנת של תפקידים, הרשאות הגישה שניתנו לכל תפקיד והגורמים המורשים ("רשימת ההרשאות התקפות").

3.9. זיהוי ואימות. נותן השירותים יעמוד בתנאי סעיף 9 לתקנות האבטחה וינקוט אמצעים מקובלים בהתאם לאופי מאגר המידע וטיבו כדי לוודא שהגישה למידע ולמערכות מאגר המידע נעשית בידי הגורמים המורשים לפי רשימת ההרשאות התקפות. כאשר גורם מורשה מסיים את תפקידו, נותן השירותים יבטל את השראתו וישנה מיידית את הסיסמאות למאגר המידע ולמערכותיו. כמו כן, נותן השירותים יוודא כי אופן הזיהוי ייעשה על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של הגורם המורשה (למשל באמצעות תעודה המכילה חתימה אלקטרונית מאובטחת).

3.10. <u>בקרה ותיעוד גישה.</u> נותן השירותים ינהל מנגנון תיעוד אוטומטי, אשר נתוניו יישמרו במשך שנתיים, שיאפשר ביקורת על הגישה למערכות מאגר המידע ("מנגנון הבקרה") ובכלל זה נתונים אלו: א) זהות המשתמש; ב) התאריך והשעה של ניסיון הגישה; ג) רכיב המערכת שאליו בוצע ניסיון הגישה; ד) סוג הגישה והיקפה; ו-ה) אם הגישה אושרה או נדחתה. נותן השירותים ידאג שמנגנון הבקרה לא יאפשר ביטול או שינוי של הפעלתו ושיפיץ התראות לאחראים במידה ואירע שינוי או ביטול שכזה. כמו כן, נותן השירותים יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דוח של הבעיות שהתגלו והצעדים שננקטו בעקבותיהן. נותן השירותים יידע את הגורמים המורשים בדבר קיום מנגנון הבקרה ויעמוד בתנאי סעיף 10 לתקנות האבטחה.

3.11. <u>אירוע אבטחה.</u> הפעיל יעמוד בתנאי סעיף 11 לתקנות האבטחה ויתעד, באמצעות מנגנון רישום אוטומטי, כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה ("אירוע אבטחה"), יודיע על אירוע האבטחה לחברה ולרשם מאגרי המידע וידווח לרשם אודות הצעדים שננקטו בעקבות אירוע האבטחה. רשם מאגרי המידע עשוי להורות נותן השירותים להודיע על אירוע האבטחה למתנדבים שנפגעו בעקבותיו. בנוסף, אחת לרבעון יקיים נותן השירותים דיון באירועי האבטחה שאירעו ויבחן את הצורך בעדכון נוהל האבטחה בעקבותיהם.

3.12. <u>התקנים ניידים.</u> נותן השירותים יעמוד בתנאי סעיף 12 לתקנות האבטחה ויגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות מאגר המידע בהתאם לרגישות המידע ולאמצעים הקיימים להגנה על המידע. כמו כן, נותן השירותים יאפשר חיבור התקנים ניידים או העתקת המידע להתקן הנייד תוך נקיטת אמצעי הגנה (לרבות הצפנה של המידע שהועתק להתקן הנייד) ובשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן הנייד.

3.13. <u>ניהול מאובטח ומעודכן של מערכות מאגר המידע.</u> נותן השירותים ינהל ויתפעל את מערכות מאגר המידע בהתאם לסעיף 13 לתקנות האבטחה ובאופן תקין לפי המקובל בהפעלת מערכות כאלה. בנוסף, נותן השירותים יפריד בין מערכות מאגר המידע לבין מערכות מחשוב אחרות המשמשות את נותן השירותים (לדוגמה באמצעות מערכת fire wall (חומת אש) פנימית, מערכת לחלוקת רשתות ועוד). כמו כן, נותן השירותים יערוך עדכונים שוטפים של מערכות מאגר המידע, ולא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים.

3.14. <u>אבטחת תקשורת.</u> נותן השירותים יעמוד בתנאי סעיף 14 לתקנות האבטחה יוודא כי מערכות מאגר המידע לא יחוברו לרשת האינטרנט או לכל רשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב. נותן השירותים יעביר את המידע ברשת ציבורית או האינטרנט רק לאחר הצפנת המידע המועבר. במידה וניתן יהיה לגשת למאגר המידע מרחוק באמצעות רשת האינטרנט או רשת ציבורית אחרת, נותן השירותים יעשה שימוש גם באמצעי פיזי הנתון לשיטתו הבלעדית של הגורם המורשה, כגון כרטיס חכם.

3.15. <u>ביקורות תקופתיות.</u> אחת לשנתיים יערוך נותן השירותים ביקורת פנימית או חיצונית בהתאם לתנאי סעיף 16 לתקנות האבטחה, על-ידי גורם המוכשר לכך, לצורך ווידוא עמידת נותן

השירותים בהוראות תקנות האבטחה. נותן השירותים ידון בדוחות הביקורת שיועברו אליו בתום הביקורת ויבחן את הצורך בעדכון נוהל האבטחה בעקבותיהם.

3.16. <u>שמירת נתוני אבטחה.</u> נותן השירותים יעמוד בתנאי סעיף 17 לתקנות האבטחה וישמור את מידע אודות ניהול הרשאות גישה (סעיף 3.8), זיהוי ואימות (סעיף 3.9), אירועי אבטחה (סעיף 3.11) ואבטחת תקשורת (סעיף 3.14) למשך שנתיים ויגבה נתונים אלו באופן שיבטיח שיהיה ניתן בכל עת לשחזר אותם למצבם המקורי.

3.17. <u>גיבוי ושחזור.</u> נותן השירותים יעמוד בתנאי סעיף 18 לתקנות האבטחה ויקבע במסמך: א) נהלים לביצוע גיבוי ואבטחת שחזור כמפורט בסעיף 3.16 לעיל; ו-ב) כי במסגרת תיעוד אירועי אבטחה על-פי האמור בסעיף 3.11 לעיל, יתועדו גם הליכי שחזור המידע ובכלל זה זהותו של מבצע הליכי השחזור ופרטי המידע ששוחזר. כמו כן, נותן השירותים ישמור את עותק הגיבוי של הנתונים כאמור בסעיף 3.16 לעיל ושל הנהלים להבטחת שחזור נתונים אלה באופן שיבטיח את שלמות המידע ואת אפשרות השחזור במקרה של אבדן או הרס.

4. **<u>מיקור חוץ</u>**

4.1. <u>העברת מידע.</u> נותן השירותים לא יעביר לצדדים שלישיים את המידע לכל מטרה אחרת שאינה המטרה.

4.2. <u>גורמים מורשים.</u> מבלי לגרוע מהאמור בסעיפים 3.7-3.9 לעיל, נותן השירותים ינקוט באמצעי הזהירות הנדרשים על-מנת לוודא שהגישה למידע ניתנת אך ורק לעובדים מורשים של נותן השירותים הצריכים גישה זו לצורך מימוש המטרה ("גורמים מורשים"). על נותן השירותים להבטיח כי השימוש במידע יהיה מידתי ולצורך המטרה בלבד. נותן השירותים ידריך את הגורמים המורשים במטרות השימוש במידע. שימוש במידע לכל מטרה אחרת יהווה הפרה יסודית של ההסכם ושל התחייבות זו. נותן השירותים לא יעביר מידע לצד ג' כלשהו לרבות קבלני משנה ללא אישור מראש ובכתב מהחברה.

4.3. <u>סודיות.</u> מבלי לגרוע מהתחייבות נותן השירותים לשמירה על סודיות המצורף כנספח ז' להסכם, נותן השירותים יוודא שבטרם מתן גישה למידע, כל הגורמים המורשים יהיו חתומים על התחייבות לשמירה על סודיות שתעמוד בחובות הסודיות בסעיף 16 לחוק.

4.4. <u>אכיפה ודיווח.</u> נותן השירותים יוודא שהוראות התחייבות זו יאכפו באופן שוטף ויעביר הדרכות ויעדכן את הגורמים המורשים אודות המטרה והשימוש במידע. בנוסף, נותן השירותים, על-פי בקשתה הסבירה של החברה, ידווח לחברה לגבי עמידתו באמצעי האבטחה, בהסכם ובהתחייבות זו.

4.5. <u>תיעוד.</u> נותן השירותים ישמור תיעוד לעניין ציות להוראות התחייבות זו, לרבות ומבלי לגרוע לגבי חקירות ובדיקות של תלונות או הפרות אפשריות של התחייבות זו. נותן השירותים יציג את התיעוד האמור בפני החברה לפי דרישה ו/או בפני הרשות להגנת הפרטיות כפי שנדרש על-פי החוק או התחייבות זו.

4.6. ביטוח. מבלי לגרוע מאחריות נותן השירותים על-פי ההסכם, התחייבות זו ו/או על-פי כל דין, נותן השירותים מתחייב, כי בכל משך תקופת ההסכם, יקיים, יערוך ויחזיק בידיו, על חשבונו ביטוחים כמפורט באישור עריכת ביטוח המצורף להסכם כנספח ו'.

4.7. שימוש לא חוקי. בשום אופן הנותן השירותים לא יאסוף, יעבד או ישתמש במידע או במאגר המידע למטרות לא מורשות או לא חוקיות.

4.8. ביקורת אבטחה. החברה ו/או הרשות להגנת הפרטיות יהיו רשאיות לבצע ביקורות תקופתיות אצל נותן השירותים, על-מנת לוודא כי נותן השירותים מקפיד לקיים את הוראות ההסכם ואת ההנחיות והדרישות המפורטות בהתחייבות זו וכן את הוראות הדין החל, וזאת בתיאום מראש עם נותן השירותים.

4.9. ביקורת באתר. נותן השירותים יאפשר לחברה ו/או לרשות להגנת הפרטיות לבצע ביקורות, לרבות ביקורות פתע, באתרי נותן השירותים שבהם נעשה שימוש במידע. במסגרת ביקורות אלו נותן השירותים ייתן לחברה ו/או לרשות להגנת הפרטיות גישה לכל חומר מחשב, אמצעי אחסון אלקטרוני או מכשיר שבו המידע מאוחסן ו/או מעובד.

4.10. הפרדת מידע. במקרה שבו נותן השירותים מספק שירותים בקשר עם מאגרי מידע של צדדים שלישיים, נותן השירותים יוודא שישנה הפרדה פיזית ו/או לוגית בין המידע לבין מידע של צדדיים שלישיים אלו. לבקשת החברה ובכפוף לאישור בכתב, נותן השירותים ימנה איש קשר אחראי על כל עניין שקשור לשימוש במידע ואבטחת המידע. לבקשת החברה, נותן השירותים ישמר הפרדה מבנית בתוך התאגיד שלו על-מנת לצמצם ככל הניתן סיכון לשימוש במידע לצרכיו האחרים.

4.11. שמירת המידע. נותן השירותים ימחק מרישומיו ומאגריו כל מידע או חלק ממנו שאינו נחוץ למטרה והכל בהתאם להוראות החברה. במקרה שבו יש דרישה על-פי חוק לשמור חלק מהמידע, אזי מידע זה יישמר בנפרד פיזית או לוגית, מכל מידע אחר, באופן שבו ימזער אפשרות לשימוש בלתי מורשה ותנאי התחייבות זו ימשיכו לחול לגבי מידע זה. עם מחיקה של המידע לאחר סיום או ביטול ההסכם, יספק נותן השירותים לחברה הצהרה חתומה על-ידי מורשה החתימה של נותן השירותים שמאשרת כי המידע נמחק.

4.12. מסמך אבטחת מידע מיקור חוץ. נותן השירותים יעמוד בדרישות מסמך אבטחת מידע מיקור חוץ של החברה, כאשר העתק של מסמך זה יהיה נגיש לנותן השירותים מיד לאחר חתימת התחייבות זו, ויהווה חלק בלתי נפרד מהתחייבות זו. מסמך אבטחה זה יתייחס בין היתר לנושאים הבאים: א) אבטחה פיזית; ב) אבטחה לוגית; ג) הפרדה של המידע; ד) מדיניות לעניין סיום השימוש במידע והסרת ציוד אחסון המידע; ה) תהליכים שקשורים למיון המידע; ו) נגישות שליטה; ז) חובות סודיות של גורמים מורשים; ח) ביקורת; ט) גיוס עובדים ובדיקות רקע (בין היתר, בנוגע להכשרת עובדים בעניין חובות זהירות בהקשר למידע), ו-י) ציות להוראות אבטחה נוספות, כולל אלו הכלולים בת"י ISO 27001 או בתקן אחר שאינו פחות מחמיר.

5. **מבלי לגרוע מן האמור בנספח ח' זה, נותן השירותים יעמוד גם בהוראות דרישות אבטחת מידע עבור מכרז נעים לירוק המצורף להתחייבות זו כמוסף ג' לנספח זה.**

6. **נותן השירותים ישפה את החברה ומי מטעמה, כולל ומבלי לגרוע את כל בעליה, מנהליה, בעלי המשרה, הגורמים הקשורים אליה ועובדיה נגד כל אבדן, הוצאה, עלויות, תביעות, פיצויים (כולל הוצאות סבירות בשל שכר טרחת עו"ד, תעריפי מומחים וכל הוצאה סבירה אחרת הקשורה בהתדיינות משפטית), הנובעים מ ו/או שבאופן כלשהו קשורים לתנאי התחייבות זו.**

7. **נותן השירותים מצהיר כי הוא מודע לכך שהתחייבות זו הינה חלק בלתי נפרד מההסכם וכי כל הפרה של התחייבות זו תחשב כהפרה יסודית של ההסכם ותזכה את החברה בכל סעד על-פי דין.**

8. **נותן השירותים מצהיר כי הוא מודע לכך שהפרת התחייבות זו עלולה לגרום לחברה נזקים חמורים ביותר ובלתי הפיכים אשר פיצוי כספי לא יהווה תרופה וסעד נאות להם, ולפיכך נותן השירותים מסכים כי החברה תהיה זכאית, במקרה של הפרת התחייבות זו, לבקש מבית משפט מוסמך להוציא נגדו צו מניעה זמני ו/או צווים אחרים במטרה למנוע ו/או להפסיק את ההפרה.**

ולראיה על החתום:

_____

[נותן השירותים]

על-ידי: _____

שם: _____

תפקיד: _____

תאריך: _____

<u>מוסף א'- נוהל האבטחה</u>

1. <u>האבטחה הפיזית והסביבתית</u> [יש לפרט הוראות לעניין האבטחה הפיזית והסביבתית של אתרי מאגר המידע, שכן תקנות האבטחה דורשות שמערכות מאגר המידע יישמרו במקום מוגן המונע חדירה וכניסה בלא הרשאה]

2. <u>הרשאות גישה למאגר המידע</u> [יש ליצור רשימת הרשאות גישה ושרשימה זו תעודכן באופן שוטף. הרשאות הגישה צריכות להינתן לפי תפקיד. הרישום יכלול את התפקיד שלו ניתנת הרשאה, את סוג הרשאת הגישה שניתנה לתפקיד זה ואת הגורמים המורשים הממלאים תפקידים אלה]

3. <u>אמצעים המגנים</u> [יש לפרט את האמצעים המגנים על מערכות מאגר המידע ואופן הפעלתם לצורך כך]

4. <u>הוראות הגנת מידע</u> [יש פרט הוראות לכלל הגורמים המורשים בנוגע להגנה על המידע]

5. <u>הסיכונים</u> [יש לפרט: את הסיכונים שחשוף להם המידע במסגרת הפעילות השוטפת של נותן השירותים, לרבות אלה הנובעים ממבנה מערכות מאגר המידע (המפורט במוסף ב' להלן); אופן קביעת סיכונים אלה; ואופן הטיפול בהם, לרבות על-ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר המידע או במערכותיו]

6. <u>אירועי אבטחת מידע</u> [יש לפרט את אופן התמודדות נותן השירותים עם אירועי אבטחת מידע בהתאם לחומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות גישה וצעדים מיידיים אחרים, וכן לעניין דיווח על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם]

7. <u>התקנים ניידים</u> [יש לפרט הוראות לעניין ניהול של ושימוש של התקנים ניידים (התקן נייד הינו כל מצא המשמש לאחסון חומר מחשב למשל מחשב נייד, disc on key וטלפון סלולארי חכם). יש להגביל/למנוע אפשרות לחיבור התקנים ניידים למערכות מאגר המידע, וזאת ייקבע בהתאם לרגישות המידע, לסיכונים המיוחדים למערכות מאגר המידע/למידע הנובעים מחיבור ההתקן הנייד ולקיומם של אמצעי הגנה מתאימים מפני סיכונים אלה. לעניין זה יראו שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד]

8. <u>זיהוי ואימות</u> [יש לפרט את אמצעי הזיהוי והאימות לגישה למאגר המידע ולמערכותיו בהתאם לאמור בסעיף 3.9 להתחייבות זו. במידה ואופן הזיהוי מבוסס על סיסמאות, על נותן השירותים להתייחס לחוזק הסיסמה, מספר הניסיונות השגויים ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד הגורם המורשה ובכל מקרה לתקופה שלא תעלה על שישה חודשים. בנוסף, על נותן השירותים להתייחס לניתוק אוטומטי של הגורם המורשה לאחר פרק זמן של אי פעילות אותו יש להגדיר כאן. כמו כן, יש להתייחס כאן לאופן הטיפול בתקלות הקשורות באימות זהות]

9. <u>הבקרה על שימוש</u> [יש לפרט את אופן הבקרה על שימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות מאגר המידע בהתאם לאמור בסעיף 3.10 להתחייבות זו]

10. <u>ביקורות תקופתיות</u> [יש לפרט הוראות לעניין עריכת ביקורת תקופתית לווידוא קיומם ותקינותם של אמצעי האבטחה בהתאם לאמור בסעיף 3.15 להתחייבות זו]

11. <u>גיבוי נתונים</u> [יש לפרט הוראות לעניין גיבוי נתונים בהתאם לאמור בסעיף 3.17 להתחייבות זו]

12. <u>פעולות פיתוח</u> [יש פרט הוראות לעניין אופן ביצוע פעולות פיתוח ותיעודן, ובכלל זה אופן הגישה של אנשי הפיתוח לנתונים במאגר המידע]

<u>מוסף ב'- רשימת מצאי של מערכות מאגר המידע</u>

1. <u>תשתיות ומערכות חומרה במאגר המידע</u> [יש לכלול את סוגי רכיבי תקשורת ואבטחת מידע]
2. <u>מערכות התוכנה במאגר המידע</u> [יש לפרט מערכות המשמשות להפעלת מאגר המידע, לניהולו, לתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו]
3. <u>תוכנות וממשקים</u> [יש לפרט את התוכנות והממשקים המשמשים לתקשורת אל מערכות מאגר המידע]
4. <u>תרשים הרשת שמאגר המידע פועל בו</u> [יש לכלול את תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של רכיבים אלה].

מסמך זה עודכן לאחרונה בתאריך: [*יש למלא את התאריך האחרון בו עודכן מסמך זה*]

מוסף ג'- דרישות אבטחת מידע עבור מכרז נעים לירוק

1. **<u>כללי</u>**

מסמך זה מציג את דרישות אבטחת מידע לנותן שירותי ניהול, תיאום, פיקוח ובקרה לניסוי "נעים לירוק 3".

2. **<u>רגולציה ומשפט</u>**

נותן השירות ימנה ממונה הגנת סייבר ואבטחת מידע – מצוות אבטחת המידע של נותן השירות ובעל הכשרה מתאימה שאחראי על הגנת סייבר ואבטחת המידע הנכלל במאגרי המידע של המזמין המאוחסנים במערכות ובשרתי נותן השירות כנדרש בחוק הגנת הפרטיות התשמ"א 1981 ותקנות אבטחת המידע.

ממונה אבטחת המידע יהיה אחראי על יישום ההנחיות של תחום סייבר בנושאי הגנת סייבר ואבטחת מידע.

ממונה אבטחת המידע של נותן השירות יעמוד בקשר שוטף עם תחום אבטחת המידע אצל המזמינה.

3. **<u>עמידה בתקני אבטחת מידע</u>**

על נותן השירות לעמוד בתקני אבטחת מידע הבאים:

- תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז - 2017, בכל הנוגע לניהול מאגרי מידע הכוללים מידע אישי.
- ככל שנותן השירות יבסס את המערכות המרכזיות על שירותי ענן, המסופקים ע"י קבלן משנה, על הקבלן לעמוד בתקן 270001. יועדפו ספקים התומכים CSA STAR . כמו כן, שמירת מאגרים, שעליהם חלים תקנות הגנת הפרטיות תהיה רק במדינות שבהן מותר להחזיק מאגרים אלו, בהתאם לתקנות הנ"ל.

4. **<u>אישור עובדים</u>**

לכלל העובדים, אשר יהיו נגישים למידע של המזמין ושל המתנדבים, יבוצע מבדק אמינות ממוחשב.

רק עובדים שיאושר בסיום תהליך זה יורשו לפעול במערכת.

המזמין יהיה רשאי לדרוש החלפת כל עובד, שלגביו יתעורר חשש כי איננו עומד בתנאים ובסטנדרטים, עליהם מחויב המזמין.

5. **<u>שימוש ברכיבי אבטחת מידע</u>**

נותן השירות יעשה שימוש ברכיבי אבטחת המידע הבאים, לכל הפחות:

- התקני firewall, שישמשו לחציצה בין רשתות בסיווגים שונים, לחיבור לרשת ה-Internet וגורמים חיצוניים ולחציצה בין משתמשים ושרתים.
- התקני WAF, להגנת אתרי WEB.
- התקני IPS, להגנת הקישור לרשת ה-Internet.

- התקני DLP, למניעת הוצאת מידע שאיננו מאובטח אל מחוץ לרשת.
- תוכנות אנטי-וירוס, לכלל העמדות והשרתים ברשת.
- מערכת NAC, למניעת גישה בלתי מורשת לרשתות נותן השירות.
- מערכת SIEM, לאיסוף, ניטור וניתוח אירועי אבטחת מידע.

6. <u>אבטחת מידע בתנועה</u>

נותן השירות נדרש להעביר מידע אשר נמצא בתנועה כגון מידע העובר בין מערכות המפעילים למערכות נותן השירות, בין מערכות נותן השירות למערכות החברה ובין מערכות נותן השירות ליישום הסלולרי, על גבי תווך תקשורת מוצפן לפחות אחד מאלה: (SSL/IPSEC/VPN/SSH וכו').

נותן השירות יידרש לאבטח את המערכת על ידי אמצעים להגנה מפני מתקפות מסוג DDOS תשתיתי ואפליקטיבי.

נותן השירות יספק פתרון אבטחה מתקדם המספק יכולות מתקדמות של ניטור ובקרה, מניעת פעילות זדונית בזמן הזיהוי, הצפנה במנוחה/תנועה, יכולות תיעוד ומעקב אחר פעולות ושינויים ויכולות אבטחה נוספות הנכללות בפלטפורמה זו.

7. <u>אבטחת נתונים נייחים</u>

נותן השירות יאפשר לחברה להצפין מידע רגיש תוך שימוש באלגוריתם הצפנה סטנדרטי ומוכר. מידע רגיש הינו מידע המוגדר כרגיש על פי חוק הגנת הפרטיות התשמ"א 1981 או שהוגדר כך על-ידי המזמין.

על נותן השירות להציג בפני המזמין את ארכיטקטורת אחסון הנתונים כדי לאפשר לחברה לזהות סיכונים אבטחתיים ובקרות זמינות להתמודדות עם סיכונים אלו.

8. <u>אחסון וגיבוי</u>

המידע המנוהל במערכות לא ייצא מתחומי המדינות המופיעות המותרות לאחסון נתונים אישיים, על פי הנחיות הרשות להגנת הפרטיות במשרד המשפטים. אתר הגיבוי של נותן השירות יהיה כפוף לאותה הרשימה.

המערכת תגובה בתדירות שלא תפחת מאחת ליום, כאשר הגיבויים יישמרו מחוץ לאתר המחשוב העיקרי.

9. <u>בקרת גישה</u>

13.1 <u>הזדהות</u>:

על נותן השירות לתמוך בלפחות שניים מאמצעי ההזדהות הבאים:

- Something you know: סיסמה מורכבת, בעת אורך מינימלי.
- Something you have: כרטיס חכם Smart Card), RSA Token), קוד OTP (One Time Password) הנשלח באמצעות SMS או מופק דרך טלפון/התקן חכם אחר.

- Something you are: אמצעי ביומטרי כגון טביעת אצבע, רשתית עין וכדומה.

13.2 <u>סיסמאות</u>:

במידה ונעשה שימוש בסיסמאות, נותן השירות יידרש נותן השירות לעמוד במדיניות הסיסמאות הבאה:

- מורכבות סיסמה: תהיה מורכבת מ-8 תווים או יותר הכוללים אותיות קטנות וגדולות, ספרות וסימנים מיוחדים.
- תוקף סיסמה: תוקף הסיסמה יפוג לאחר תקופה של עד 90 יום ולאחר מכן יידרש המשתמש להחליפה.
- היסטוריית סיסמאות: תשמר היסטוריית סיסמאות של לפחות 10 סיסמאות לאחור.

13.3 <u>התחברות וניתוק</u>:

ניסיונות הזדהות שגויים באמצעות כל אחד משלושת שיטות ההזדהות שהוזכרו תוביל לנעילת המשתמש למשך 15 דקות.

יוגדר פרק זמן קבוע שלאחריו יופעל מנגנון ניתוק תקשורת (session time out) המחייב זיהוי מחדש של המשתמש.

10. <u>ניהול הרשאות וזהויות</u>

יש להגדיר הרשאות גישה למידע באופן מדוקדק תוך הענקת הרשאות גישה רק לגורמים אשר גישתם למידע הכרחית לצורך מילוי תפקידם.

11. <u>נגישות למידע על-ידי אנשי נותן השירות</u>

יש לצמצם את קבוצת אנשי נותן השירות היכולים לשלוף את כלל המידע למינימום.

כל פעולות ה-DBA ינטרו ברמה פרטנית ובאופן חד ערכי וכל פעילות של יצירה שינוי בבסיסי הנתונים ובמידע תועבר לצוות אבטחת המידע.

מידע של מתנדבים לא יוצא החוצה שלא בדרך שסוכמה עם המזמין.

12. <u>מעקב ובקרה</u>

רישומי המערכת ייאספו ע"י מערכת SIEM או Syslog ייעודית או ישלחו למערכת ה-SIEM של המזמין לצורך ניטור והתראה על אירועי אבטחה המתרחשים במערכות.

על ספק השירות לאפשר למזמין, או מי מטעמו לאסוף את רישומי המערכת בזמן אמת/באופן מתוזמן.

הלוגים יועברו בפורמט UTC.

נותן השירות מתחייב לשמור לאחור רישומי מערכת לתקופה המשתנה בהתאם לרגישות המערכת ולדרישות רגולטוריות התקפות למערכת.

על נותן השירות לוודא כי רישומי המערכת נשמרים בשרת מרכזי המנוהל ע"י צוות עובדים נפרד.

במקרה בו ישנה נותן השירות את מערכת הלוגים עליו לעדכן את המזמין 60 יום מראש על מנת שיוכל להיערך.

נותן השירות יידרש לבצע ניטור לשירותים ומערכות ברבדים הבאים:

- ניטור לוגים - איתור בזמן אמת או בדיעבד של בעיות טכניות או אירועי אבטחת מידע המתרחשים.
- ניטור ביצועים – מעקב אחר עומסים במשאבי המחשוב.
- ניטור ומעקב אחר פעילויות חריגות/עויינות (ניסיונות הזדהות כושלים, גישה לא מורשית, ניסיונות כניסה כפולים ועוד).

אירועים שיוגדרו ברמת סיכון גבוה כגון חשד לנגישות זרה ו/או הזלגת מידע ממאגר הנתונים נותן השירות יעדכן באופן מידי את המזמין (על פי רשימת תיוג מוגדרת) ויודיע את אופן הטיפול בהם.

13. <u>ביקורת</u>

אחת ל-18 חודשים, לכל הפחות, יבצע נותן השירות:

- מבדקי חדירה. מבדקים אלו יבוצעו ע"י חברה מתמחה ייעודית, שלא הייתה מעורבת בתהליך הקמת המערכות.
- סקר סיכונים כולל.

תוצאות הסקרים והמבדקים יוצגו למזמין בפגישה שנתית. על נותן השירות להציג תכונית לתיקון הממצאים במידה ויש. במקרה של ליקויים מהותיים המשפיעים ישירות על מערכות המזמין יש לידע באופן מידי את המזמין על המצאות הליקוי.

נותן השירות יאפשר לנציגים מטעם המזמין לקיים סיור במתקניו הרלוונטיים לשם ביקורת אבטחת מידע ועמידה בהסכמים ו/או חוזים אשר נחתמו מול המזמין.

14. <u>מניעת Lockdown</u>

נותן השירות יאפשר לחברה לשמור עותק מקומי של כל מידע בחצרות המזמין ו/או בכל אתר אחר של החברה.

15. <u>סיום התקשרות עם ספק</u>

עם סיום ההתקשרות עם נותן השירות, על נותן השירות מוטלת האחריות לבצע את הפעולות הבאות:

- מחיקה חד חד ערכית ולא ניתנת לשחזור של כל הנתונים והמידע השמורים במערכות.
- השמדת עותקים של הנתונים והמידע בהם נעשה שימוש במסגרת פעילות נותן השירות עבור המזמין.
- דרישה מנותן השירות להציג הוכחות לכך שהמידע הושמד (רישומים ודוחות רלוונטיים).
- במידה והמידע הוצפן –ביטול (Revoke) מפתחות ההצפנה ומחיקתם.