

## נספח השמירה על הפרטיות

נספח השמירה על הפרטיות ביחד עם כל נספחיו המצ"ב (להלן, כולם ביחד: "נספח הפרטיות") הנחתם בתאריך [ ] , 2022 ועם חתימתו על ידי שני הצדדים שלהלן יהפוך לחלק מהסכם השירותים (להלן: "הסכם השירותים") שנחתם בין [ ] (להלן: "החברה") ו-[ ] (להלן: "נותן השירותים") בתאריך [ ] .

**הואיל** תוך כדי מתן השירותים במסגרת הסכם השירותים, נותן השירותים עשוי לעבד מידע אישי (כהגדרתו להלן) עבור החברה ;  
**לפיכך** בהתחשב בהסכמים ההדדיים הכלולים בנספח פרטיות זה ובהסכם השירותים, החברה ונותן השירותים מסכימים בזה, תוך כוונה להתחייב משפטית, כדלקמן :

### 1. הצהרות והתחייבויות נותן השירותים

מבלי לגרוע מכל התחייבויותיו של נותן השירותים על פי הסכם ההתקשרות אליו מצורף נספח זה , נותן השירותים מתחייב:

- 1.1. למלא אחר הוראות הסכם השירותים, נספח הפרטיות הזה (לרבות תוספות 1 - 2) וכל חוק והנחיה בענייני פרטיות החלים על עיבוד מידע והגנת הפרטיות, לרבות, חוק הגנת הפרטיות תשמ"א-1981 (להלן: "חוק הפרטיות") והתקנות והצווים שהותקנו על פיו, תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, הנחיה 2/2011 בדבר שימוש במיקור חוץ לעיבוד מידע אישי וכל הנחיה אחרת של הרשות להגנת הפרטיות (להלן ביחד: "הדין החל") בקשר ל"מידע" כהגדרתו בדין החל (להלן "מידע אישי" או "מידע").
- 1.2. כי לא יאסוף מידע בדרכים בלתי-חוקיות, או יעשה שימוש במאגרי מידע בלתי חוקיים.
- 1.3. כי ככל שהוא אוסף מידע אישי מנושאי המידע ישירות, יפעל בהתאם להוראות סעיף 11 לחוק הגנת הפרטיות, התשמ"א-1981, ויעמוד בחובת ההודעה. במסגרת זו, נותן השירותים ימסור לנושא המידע הודעה הכוללת את כל הפרטים הנדרשים לפי החוק, לרבות: זהות הגורם האוסף את המידע, המטרות לשמן נאסף המידע, האם חלה חובה חוקית למסור את המידע או שמסירתו היא וולונטרית, מי הם הגורמים שאליהם יועבר המידע, אם קיימים כאלו. כמו כן, נותן השירותים מתחייב להימנע משימוש במידע אישי שנאסף למטרות שאינן אלו שהובאו לידיעת נושא המידע, אלא אם קיבל לכך את הסכמתו המפורשת של נושאי המידע, בהתאם לדרישות החוק.
- 1.4. מבלי לגרוע מהאמור בסעיף 1.3 מעלה, מתחייב נותן השירותים כי המידע אשר יועבר וילא במהלך ההתקשרות ישמש לצורך ביצוע השירותים ולמטרות חוקיות, בהתאם למטרות המוגדרות לכך בהסכם ובהתאם להוראות הדין תוך נקיטת אמצעים מספקים להבטחת פרטיותם של נושאי המידע .
- 1.5. שלא להעביר את המידע האישי לכל אדם או גוף אחר, ו/או לא להשתמש באף קבלן משנה עבור עיבוד המידע, הן במדינת מושבו והן במדינות אחרות, ללא הסכמה מפורשת מראש ובכתב מאת החברה.
- 1.6. לעבד את המידע רק עבור מתן השירותים במסגרת הסכם השירותים ונספח הפרטיות ולשמור על סודיות המידע.
- 1.7. לקיים בקורות ארגוניות ותוכניות הכשרה להכשיר את אלה מבין עובדיו ואנשי הצוות שלו שהורשו לגשת ולעבד את המידע האישי כדי להבטיח ציות להסכם השירותים, לנספח הפרטיות ולדין החל.
- 1.8. לתעד את פעילותו ואת הליכי קבלת החלטות שלו המתייחסים ליישומו של נספח הפרטיות.
- 1.9. לספק לחברה דו"חות אודות ניהול ועיבוד של המידע האישי ובנוגע לכל ענייני האבטחה. דו"חות אלו יסופקו לפחות פעם אחת בשנה. נותן השירותים ידווח לחברה באופן מידי על כל אירוע חריג.
- 1.10. נותן השירותים מאשר ומסכים כי החברה הינה הבעלים הבלעדיים של כלל המידע האישי שייאסף או יעובד על ידי נותן השירותים עבור החברה או המידע שיועבר על ידי החברה לנותן השירותים ושל תוצרי העיבוד של מידע זה. החברה זכאית להנחות את נותן השירותים בקשר לעיבוד המידע האישי.

1.11. נותן השירותים מאשר ומסכים כי תנאי נספח הפרטיות, לרבות עניין אבטחת המידע, הינם תנאים מהותיים בהתקשרותו עם החברה.

## **2. עיבוד מידע אישי על ידי נותן השירותים**

2.1. נותן השירותים לא יאסוף מידע אישי ישירות מנושאי המידע.

2.2. אסור באיסור מוחלט לנותן השירותים לאסוף ו/או לעבד מידע שהתקבל ממקורות בלתי חוקיים.

2.3. הרשאת גישה למידע אישי תינתן אך ורק לאנשים אשר תפקידם מחייב גישה למידע אישי, אשר מחויבים על פי דין או הסכם לשמור על פרטיות המידע ואך ורק לצורך ביצוע השירותים והמחויבויות המפורטות בהסכם זה. רשימת משרות אצל נותן השירותים וסוגי אנשי צוות שתהיה להם גישה למידע אישי, וכן רמות הגישה המותרת רשומים בתוספת 1.

## **3. שמירה והחזרה של מידע אישי**

3.1. נותן השירותים מתחייב כי ישמור על כל המידע שיתקבל מהחברה ו/או אגב מתן השירותים ו/או לצורך ביצוע הסכם זה, רק למשך פרק הזמן הנדרש במישרין לביצוע השירותים על פי ההסכם. ככל שקיימת הוראה בדין המחייבת את שמירת המידע אצל הספק, הספק מתחייב בזאת לוודא כי אמצעי האבטחה והבקרה שהוגדרו בהסכם זה יישארו אפקטיביים לכל אורך תקופת השמירה.

3.2. נותן השירותים ישמור את המידע האישי שנאסף עבורו או בשם החברה כל עוד יש צורך בכך על מנת להגשים את המטרות שלשמן הועבר לנותן השירותים בלבד.

3.3. נותן השירותים יחזיר, ימחק או יבער את כל המידע האישי, לרבות כל העותקים הנמצאים על כוננים קשיחים, אמצעי גיבוי, וכל מדיה מגנטית או אופטית אחרת מיד לאחר בקשת החברה בכתב או בסיום הסכם השירותים ו/או נספח פרטיות זה, לפי המוקדם ביניהם.

3.4. נותן השירותים יספק לחברה, לבקשתה, תצהיר על פיו כל המידע האישי כאמור נמחק או הושמד. ככל שיהיה צורך לשמור עותק מהמידע האישי לצורך התגוננות בפני הליכים משפטיים, נותן השירותים יפקיד עותק של המידע בידי נאמן מוסכם.

3.5. ככל שנדרשת על ידי נותן השירותים זכות גישה למידע לאחר סיום ההתקשרות לצורך התגוננות בפני תביעות בקשר עם תפקידיו לפי ההסכם או לצורך חוקי אחר, אזי ישמור נותן השירותים עותק של המידע באמצעי גיבוי מקובל אצל צד ג' נאמן אשר יהיה רשאי להתיר את הגישה למידע אך ורק למטרות הנ"ל.

## **4. זכויות עיון ותיקון של נושאי המידע**

נותן השירותים יסיע לחברה כדי שתוכל למלא אחר דרישות הדין החל בנושא עיון ותיקון של המידע האישי על ידי נושאי המידע. אם נושא המידע ו/או נציגו המורשה יגיש בקשה בכתב לנותן השירותים לעיין במידע האישי שלו, כי אז נותן השירותים: (א) תוך יומיים מקבלת בקשה כאמור יודיע לנושא המידע באם נותן השירותים מעבד את המידע האישי שלו ולא ימסור לו כל מידע נוסף (למעט האמור בס"ק (ב) להלן); (ב) ימסור לנושא המידע את שם החברה ואת הכתובות לפניות נוספות; ו-(ג) תוך יומיים יודיע לחברה בכתב אודות הפנייה בצירוף הפרטים הרלוונטיים. היה ויתברר כי המידע האישי אינו מדויק, אינו שלם או אינו עדכני, יבצע נותן השירותים את התיקונים, כפי שתורה לו החברה ויודיע לחברה בכתב על תיקון המידע האישי מייד כשיבוצע.

## **5. אבטחת המידע האישי**

5.1. נותן השירותים מצהיר ומתחייב ליישם אמצעי אבטחה אדמיניסטרטיביים, טכניים, ופיזיים ואמצעי אבטחה אחרים ההולמים את סוג המידע האישי המעובד על ידי נותן השירותים עבורו ובשם החברה, ולסיכון של פגיעה באבטחת מידע כמפורט בתוספת 2.

5.2. נותן השירותים מצהיר ומתחייב כי הוא מעסיק אצלו ממונה אבטחת מידע, אשר אחראי על קיום דרישות החוק ויישום חובות נותן השירות כפי שהן באות לידי ביטוי בהסכם ובנספח זה.

5.3. נותן השירותים מתחייב לפעול כך שנתונים ומידע אשר יועברו אליו בהתאם להסכם זה, יאובטחו במידה המקובלת והסבירה, כך שלא תתאפשר גישה, בין באופן אקטיבי ובין באופן פאסיבי, למידע ולנתונים אלו, לאיש מלבד המורשים לכך

5.4. מבלי לגרוע מהאמור, נותן השירותים ימלא אחרי תקן ISO 27001 ויחזיק את המידע האישי המעובד עבור החברה בתיקיות נפרדות ממידע המעובד עבור צדדים שלישיים, לרבות אך ללא הגבלה, של לקוחות אחרים של נותן השירותים, וימנה ממונה אבטחה ככל שהדבר ידרש על פי הדין החל ויעשה את כל הדיווחים לרשם מאגרי המידע הנדרשים על פי הדין החל.

5.5. נותן השירותים יודיע לחברה בכתב על כל פגיעה באבטחת המידע המשפיעה על המידע האישי המעובד על ידי נותן השירותים עבור או בשם החברה מידית. כל הודעה כאמור תכלול פירוט מספק של השפעת הפגיעה על החברה ועל נושאי המידע. נותן השירותים יעזור בצורה סבירה לחברה בחקר האירוע וינקוט בכל אמצעי התיקון הדרושים והמתאימים.

## 6. זכויות פיקוח ובקרה

6.1. נותן השירותים ימציא לבקשת החברה אישור על-פיו קיים את חובותיו בהתאם לנספח פרטיות זה.

6.2. החברה תהא רשאית במהלך תקופת הסכם זה, ועל חשבונה לבצע מעקב וביקורות שוטפות, לבדיקת פעילותו של נותן השירותים בכל הקשור לביצוע השירותים כהגדרתם בהסכם זה לעיל. לצורך כך, נציג מטעם החברה יהא רשאי להיכנס למשרדי נותן השירותים ו/או ספקי המשנה בשעות העבודה המקובלות, ובליוי נציג מטעם נותן השירותים, ולבדוק את תקינות נהלי האבטחה ביחס להסכם זה, וכן את קיום הוראות הסכם זה בכללותו, לרבות בדיקת חומרים במחשבי נותן השירותים, ככל שאלו קשורים למידע אשר נמסר על-ידי החברה או הקשורים ישירות לביצוע השירותים. המועד לקיום הביקורות השוטפות יהיה בתיאום עם נותן השירותים, לפחות שבעה (7) ימי עסקים מראש. במקרים מתאימים ובהתאם לרגישות המידע, החברה רשאית לבצע ביקורות פתע על מנת למלא אחר הדין החל.

6.3. החברה רשאית לערוך אצל נותן השירותים, בכפוף לשיקול דעתה הבלעדי ובתאום מראש, סקר אבטחת מידע על-מנת לוודא כי נותן השירותים מקיים את התחייבויותיו על-פי נספח פרטיות זה.

6.4. החברה תהא רשאית, לפי דרישתה, לקבל מנותן השירותים דיווחים בכל הנוגע לאופן ניהול מאגר המידע שלו ועיבוד המידע שבו, וכן לקבל דיווח בכל מקרה של חשש לדליפת מידע מהמאגר או שימוש החורג מהרשאות שניתנו לשימוש בו.

6.5. החברה תהא רשאית להורות לנותן השירותים, בכתב, כל הוראה מקצועית סבירה הנראית לה, לצורך ביצוע תקין של הסכם זה ובכפוף להוראות הדין. לעניין זה, ועל אף האמור בהסכם זה, הצדדים מסכימים כי נותן השירותים לא יהיה אחראי לכל נזק ו/או תוצאות בקשר עם ביצוע ההוראות הכתובות של החברה כאמור.

6.6. נותן השירותים מכיר בחובותיו כלפי רשם מאגרי המידע, לרבות את זכויות הרשם לבצע פיקוח.

6.7. במשך כל תקופת הסכם זה, יהיו הצדדים לבצע שינויים במטרות השימוש במאגרים. לעניין זה, מוסכם בין הצדדים, כי כל שינוי במטרות השימוש במאגרים חייב להיעשות בכתב ובאופן הדדי, בין האחראי על ביצוע הסכם זה בין החברה לנותן השירותים.

## 7. סעיף: מינוי אנשי קשר ותיאום בין הצדדים

7.1. כל אחד מהצדדים ימנה איש קשר מטעמו, אשר ישמש כאחראי לתקשורת ותיאום בכל הנוגע להסכם זה.

7.1.1. איש הקשר מטעם החברה: \_\_\_\_\_

7.1.2. איש הקשר מטעם נותן השירותים: \_\_\_\_\_

**7.2. תחומי אחריות אנשי הקשר :**

7.2.1. תיאום וקביעת נהלים ותהליכים להדרכת עובדי נותני השירותים לצורך הטמעת השירות בהתאם לדרישות המזמין.

7.2.2. טיפול בבירורים ותיאום בכל הנוגע לשימוש המותאם במידע האישי ולהבטחת עמידה בדרישות החוק ובנהלים שנקבעו בין הצדדים.

7.2.3. מתן מענה לשאלות או בעיות המתעוררות במהלך ביצוע ההסכם, כולל טיפול בנושאים טכניים או תפעוליים הקשורים להטמעת השירות והשימוש בו.

7.3. **תקשורת ותיעוד:** אנשי הקשר יקיימו תקשורת שוטפת, יערכו ישיבות עבודה לפי הצורך ויתעדו את החלטותיהם וסיכומיהם בכתב, תוך שמירת עותקים בהתאם לדרישות הצדדים.

7.4. **עדכון איש קשר:** כל צד יהיה רשאי להחליף את איש הקשר שמונה מטעמו, ובלבד שימסור על כך הודעה בכתב לצד השני לפחות [מספר ימי הודעה] ימים מראש, תוך ציון פרטי איש הקשר החדש.

**8. ביטוח ושיפוי**

נותן השירותים יערוך ויקיים על חשבונו פוליסת ביטוח בגין חבות מקצועית ויצרף את החברה כמבוטח נוסף. נותן השירותים ישפה את החברה ו/או את נושאי המשרה, הדירקטורים, את העובדים או מי מטעמן, בגין כל הוצאה, עלות או חבות הנובעות מהפרת איזה מן ההתחייבויות של נותן השירותים על פי נספח פרטיות זה או על פי הדין החל.

**9. סיום ההתקשרות והדין החל**

החובות של נותן השירותים לפי נספח פרטיות זה יחולו כל עוד הוא מספק שירותים לחברה ו/או יש לו גישה למידע האישי. תנאי סעיפי 7 ו-8 בנספח פרטיות זה ימשיכו לחול גם לאחר פקיעתו או סיומו של נספח הפרטיות ו/או הסכם השירותים. הצדדים מסכימים בזאת כי הדין החל על הסכם זה הנו הדין הישראלי. כל סכסוך הנובע מהסכם זה או בקשר עימו יידון על-ידי בתי המשפט המוסמכים בתל אביב-יפו בלבד. נותן השירותים מכיר בכך כי כל הפרה ממשית או צפויה של הסכם זה עלולה לגרום לנזק בלתי הפיך לחברה, ומשכך במקרה של הפרה כאמור תהיה החברה רשאית לדרוש כל צו ו/או כל סעד אחר מהיושר מכל בית משפט בעל סמכות.

**ולראיה באו הצדדים על החתום:**

[ \_\_\_\_\_ ]

[ \_\_\_\_\_ ]

תאריך \_\_\_\_\_

תאריך \_\_\_\_\_

שם \_\_\_\_\_

שם \_\_\_\_\_

תפקיד \_\_\_\_\_

תפקיד \_\_\_\_\_

חתימה \_\_\_\_\_

חתימה \_\_\_\_\_

**תוספת 1**

**עיבוד מידע**

	רשימת משרות אצל נותן השירותים וסוגי אנשי צוות שתהיה להם גישה למידע אישי, וכן רמות הגישה המותרת
	סוגי מידע שיועבדו על ידי נותן השירותים
	מטרת עיבוד המידע
	סוגי העיבוד המותרים
	מערכות להן תינתן גישה לנותן השירותים
	סוגי הסיכונים העיקריים בקשר לעיבוד המידע
	איש הקשר של נותן השירותים לכל עניין הקשור לנספח הפרטיות יהיה.
	איש הקשר של החברה לכל עניין הקשור לנספח הפרטיות יהיה

## תוספת 2

### אבטחת מידע

**מאגר המידע של החברה הינו מאגר ברמת אבטחה [בסיסית/בינונית/גבוהה] ולכן החובות החלות עליו הינן החובות בטור [בסיסי/בינוני/גבוה]**

בסיסי	בינוני	גבוה	
<p>תותן השירותים יתעד, באופן אוטומטי במידת האפשר, כל אירוע המעלה חשש לפגיעה בשלמות המידע או לשימוש בו בלא הרשאה או לגישה למאגר ללא הרשאה (להלן: "אירועי אבטחה")</p>	<p>כמו כן, יתועדו צעדים שננקטו לשחזור מידע, זהות מבצע הצעדים ופרטי מידע שאוחזר.</p>	<p>זהה למאגר מידע ברמת אבטחה בינונית.</p>	<p><b>תיעוד אירועי אבטחה</b></p>
<p>אין</p>	<p>אחת לשנה יבוצעו ביקורות אירועי אבטחה, על מנת להעריך אם נדרש לבצע שינויים בנהלי אבטחת המידע</p>	<p>ביקורת אירועי אבטחה יבוצעו אחת לרבעון.</p>	<p><b>ביקורות אירועי אבטחה תקופתיות</b></p>
<p>תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע יוחזקו במקום פיזי המונע גישה בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע בו.</p>	<p>כמו כן, יינקטו אמצעים לבקרה ולתיעוד של הכניסה והיציאה של אנשים וצידוד מהאתר הפיזי שבו נמצא מבנה המערכת.</p>	<p>זהה למאגר מידע ברמת אבטחה בינונית.</p>	<p><b>אמצעי אבטחה פיזיים</b></p>
<p>מערכות המאגר לא יחוברו לרשת האינטרנט או לרשת ציבורית אחרת, בלא אמצעי הגנה מתאימים מפני חדירה בלתי מורשית ווירוסים, כגון חומות אש ותוכנות אנטי וירוס.</p> <p>העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בטכנולוגיית הצפנה מקובלת.</p> <p>במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, ייעשה שימוש באמצעי אבטחה נוספים על מנת להבטיח כי רק בעלי הרשאה נכנסים למאגר המידע, ואך ורק בהתאם להרשאתם.</p>	<p>כמו כן, הגישה תבוצע באמצעים פיזיים הנתונים לשליטתו הבלעדית של בעל הרשאה (כגון, לדוגמה, באמצעות כרטיסי זיהוי חכמים).</p>	<p>זהה למאגר מידע ברמת אבטחה בינונית.</p>	<p><b>אמצעי אבטחה טכניים</b></p>

<p>כני"ל</p>	<p>כני"ל</p>	<p>רכיבי מערכות מחשב המאפשרים גישה למידע במאגר יופרדו, במידת האפשר, מרכיבי מערכות המחשב האחרים. עדכונים שגרתיים יבוצעו במערכות הרלבנטיות, לרבות בתוכנה, לפי הצורך. לא ייעשה שימוש במערכות שהיצרן לא מספק להן תמיכת אבטחה, אלא אם כן ניתן מענה אבטחתי חלופי מתאים.</p>	<p><b>אמצעי אבטחה אחרים</b></p>
<p>זהה למאגר מידע ברמת אבטחה בינונית. כמו כן, נותן השירותים אחראי לכך שישמרו עותקי הגיבוי ושל הנהלים, באופן שיבטיח את שמירת או יכולת שחזור מידע הכניסה בשלמותו.</p>	<p>מאגרי מידע יגובו באופן שיבטיח את שחזור מידע הכניסה למצבו המקורי, בכל עת. על נותן השירותים להחזיק מסמך הקובע:</p> <ul style="list-style-type: none"> <li>• נהלים לביצוע גיבויים תקופתיים קבועים</li> <li>• נהלים לשחזור מידע, שיבוצעו אך ורק באישור מנהל המאגר</li> <li>• תיעוד אירוע האבטחה יכלול גם הליכי שחזור מידע, וכן את זהות מי שביצע את הליכי השחזור</li> </ul>	<p>אין</p>	<p><b>גיבוי ושחזור</b></p>
<p>כני"ל</p>	<p>כני"ל</p>	<p>שימוש בהתקנים ניידים למערכות המאגר יצומצם במידת האפשר, בהתחשב ברגישות המידע, רמת האבטחה של המאגר והסיכונים הנוגעים לו. אם תותר גישת התקנים ניידים, על נותן השירותים לנקוט אמצעי הגנה בשים לב לאמור לעיל. הצפנת מידע מקובלת בהתקנים ניידים תיחשב כנקיטת אמצעים סבירים להגנת המידע.</p>	<p><b>גישת התקנים ניידים</b></p>
<p>זהה למאגר מידע ברמת אבטחה בינונית. כמו כן, ניתן לבצע את החובות לעיל במסגרת סקר הסיכונים המבוצע אחת ל-18 חודשים, כמפורט להלן. נותן השירותים ברמת אבטחה גבוהה יבצע:</p> <ul style="list-style-type: none"> <li>• סקר סיכונים לזיהוי סיכוני אבטחת מידע לפחות אחת ל-18 חודשים. על נותן השירותים לטפל בכל אי התאמה שנתגלתה בביקורות כאמור, ולקבוע האם תוצאות הביקורת מצביעות על צורך לתקן</li> </ul>	<p>נותן השירותים אחראי לכך שתיערכנה ביקורות חיצוניות או פנימיות על ידי עובדים מוסמכים, על מנת לוודא ציות לתקנות אבטחת המידע. ביקורות אלו יבוצעו אחת ל-24 חודשים ולא יבוצעו על ידי ממונה אבטחת המידע. הביקורת תכלול דוח בכתב המתעד ציות או אי ציות לתקנות אבטחת המידע ולמדיניות אבטחת המידע, תזהה ליקויים ותציע אמצעי תיקון במידת הצורך. נותן השירותים יעיין בדוח ויקבע אם ישנו צורך לעדכן את מסמך הגדרות המאגר ומדיניות אבטחת המידע.</p>	<p>אין</p>	<p><b>דרישות בקרה ובדיקות</b></p>

<p>את מסמך הגדרות המאגר או את מדיניות אבטחת המידע.</p> <ul style="list-style-type: none"> <li>מבדקי חדירות למערכות המאגר, לצורך קביעת יכולתה של המערכת להתגונן מפני סיכונים פנימיים וחיצוניים, יבוצעו לפחות אחת ל-18 חודשים. על נותן השירותים לטפל בכל אי התאמות שנתגלו במבדקים כאמור.</li> </ul>			
<p>זהה למאגר מידע ברמת אבטחה בינונית.</p>	<p><u>כמו כן</u>, הכשרה בנוגע למדיניות אבטחת המידע ותקנות אבטחת המידע וכן דרישות רלבנטיות אחרות בתחום אבטחת המידע, תבוצע לפחות אחת ל-24 חודשים (ולגבי הסמכה של בעל הרשאה לתפקיד חדש, סמוך ככל האפשר למועד תחילת הסמכתו).</p>	<p>דרישות למתן או להרחבת גישה למאגר מידע</p> <ul style="list-style-type: none"> <li>גישה למאגרי מידע תינתן אך ורק לבעלי תפקידים שיהיו זקוקים לכך לצורך ביצוע תפקידים ואך ורק בהתאם לדרישות התפקיד.</li> <li>נותן השירותים ינקוט אמצעים סבירים על מנת להבטיח שאין חשש שיש בו כדי למנוע גישה מהאדם הרלבנטי, תוך הבאה בחשבון של מידת רגישות המידע והיקף הגישה שניתנה לו</li> <li>נותן השירותים יקיים הדרכות לבעלי ההרשאות הרלבנטיים וימסור מידע בנוגע לחובה לציית לתקנות אבטחת המידע ולמדיניות אבטחת המידע</li> </ul>	<p><b>גישה למאגרים; בקרות גישה</b></p>
<p>זהה למאגר מידע ברמת אבטחה בינונית.</p>	<p><u>כמו כן</u>, יחולו דרישות הגישה והאימות להלן:</p> <ul style="list-style-type: none"> <li>זיהוי המשתמש ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה (לדוגמה, זיהוי טביעת אצבע)</li> <li>היה אופן הזיהוי מבוסס על סיסמאות, יש להתייחס לנקודות הבאות: <ul style="list-style-type: none"> <li>חוזק הסיסמה</li> <li>מספר הניסיונות השגויים</li> <li>תדירות החלפת הסיסמאות (לכל היותר אחת ל-6 חודשים)</li> </ul> </li> <li>ניתוק אוטומטי לאחר פרק זמן של אי פעילות</li> <li>אופן הטיפול בתקלות הקשורות באימות וזהות</li> </ul>	<p>נותן השירותים ישתמש בשיטות מקובלות על מנת להבטיח כי רק משתמשים מורשים יהיו בעלי גישה למאגר, ועליו להעמיד אמצעים לביטול ההרשאה, ובמידת הצורך, להחליף סיסמאות, למשתמשים שיש לבטל את הרשאתם להיכנס למאגר המידע.</p> <p>על נותן השירותים לנהל רשימה של בעלי תפקידים המצריכים גישה למאגר, מידת הגישה שתוענק לכל בעל תפקיד כאמור, ובעלי ההרשאות המחזיקים בתפקידים אלו נכון לאותה עת.</p>	<p><b>בקרת ומעקב הרשאות</b></p>



	<ul style="list-style-type: none"> <li>• ניהול יומני גישה אוטומטיים הכוללים: <ul style="list-style-type: none"> <li>○ זהות המשתמש</li> <li>○ תאריך ושעת ניסיון הגישה</li> <li>○ רכיב המערכת שאליו בוצע ניסיון הגישה</li> <li>○ סוג והיקף הגישה</li> <li>○ הצלחת או כישלון הגישה</li> </ul> </li> <li>• מנגנון הבקרה לא יאפשר ביטול או שינוי של הפעלתו; מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים</li> <li>• נותן השירותים יקבע נוהל בדיקה שגרתי של יומני הגישה וידווח אודות כל בעיה שנתגלתה בנוגע לכך ואודות הצעדים שנקטו לתיקונה</li> <li>• יומני גישה יישמרו למשך 24 חודשים לפחות</li> <li>• נותן השירותים יידע את בעלי ההרשאות בדבר קיום היומן האוטומטי</li> </ul>		
<p>זהה למאגר מידע ברמת אבטחה בינונית.</p>	<p>גישה מרחוק מצריכה, במידת האפשר, שימוש באמצעים פיזיים ייחודיים לבעל ההרשאה, כגון כרטיס חכם או התקן נייד, כפי שיפורט במדיניות אבטחת המידע.</p>	<p>אין הגבלה</p>	<p><b>גישה מרחוק</b></p>
<p>זהה למאגר מידע ברמת אבטחה בינונית.</p>	<p>כמו כן, תיעוד כאמור יגובה באופן שיבטיח את שחזורו למצבו המקורי, בכל עת.</p>	<p>פעולות המבוצעות לקיום הוראות תקנות אבטחת המידע יתועדו, ותיעוד כאמור יישמר לפרק זמן של 24 חודשים.</p>	<p><b>תיעוד</b></p>