נספח ב' (המשך) - דרישות אבטחת מידע מול נותן שירותים מחזיק מידע

1. ניהול אבטחת מידע בחברה

1.1. נותן השירותים יציג על פי דרישת החברה את האופן בו מנוהלת אבטחת המידע אצל נותן השירותים, נהלים הקיימים בנושא זה ומנגנוני האבטחה הפיסיים והטכנולוגיים המיושמים על ידו בנושאים שלהלן:

1.1.1. מדיניות, נהלים, תהליכים ומנגנונים התומכים בנושא אבטחת מידע בחברה.

1.1.2. יישום בפועל של אבטחת המידע במערכות הטכניות.

1.1.3. ביצוע בקרה שוטפת – לאיתור שינויים לא מבוקרים בהגדרות המערכות ולאיתור פעולות חריגות / חשודות.

1.1.4. ביצוע ביקורות תקופתיות לשם איתור חולשות כתוצאה משינויים במערך המחשוב, איומים חדשים וכדומה.

2. הצהרות סודיות וניהול כוח אדם:

2.1. כחלק מהחוזה בין החברה לבין נותן השירותים ייחתם הסכם סודיות המפרט את מחויבותו של נותן השירותים לשמירה על סודיות המידע של החברה המופקד בידיו לצורך מתן השירותים לחברה.

2.2. נותן השירותים יגדיר ויספק לחברה רשימה שמית של כל עובדיו המורשים על ידו לעסוק בפרויקטים הקשורים לחברה ולהיחשף למידע של החברה המועבר לידיו (להלן: "**צוות כלל**"). הרשימה תכיל גם את העובדים שאינם נותנים שירותים לחברה אך עשויים להיחשף למידע במסגרת הרשאותיהם (לדוגמא – מנהל רשת).

2.3. אחד החברים הבכירים בצוות יוגדר כנאמן אבטחת המידע של החברה אצל נותן השירותים, וישמש כאיש הקשר העיקרי מול מנהל אבטחת המידע של החברה. במידה וקיים אצל נותן השירותים מנהל אבטחת מידע מוגדר – יוכל הוא לשמש כאיש הקשר לטובת העניין גם אם אינו חבר בצוות ובתיאום בינו לבין מנהל אבטחת המידע של החברה יוגדר הצורך בנאמן אבטחת מידע נוסף.

2.4. העובדים הנמנים על "צוות כלל" יהיו חתומים, ללא תלות בהסכם בין החברות, על הסכם סודיות אישי זהה לזה שחותמים עליו עובדי חברה ועובדי מיקור חוץ בחברה. לשם כך יעודכן מנהל אבטחת המידע בחברה אודות שינויים ב"צוות כלל" (הצטרפות עובדים חדשים לצוות, פרישה של עובדים מהצוות ו/או סיום העסקתם אצל נותן השירותים).

2.5. על נותן השירותים להדריך את עובדיו במטרות השימוש במידע ויוכיח את קיום ההדרכות לחברה.

2.6. במסגרת הליכי קליטת עובדים חדשים אצל נותן השירותים, וב"צוות כלל" בפרט, החברה ממליצה על קיום בדיקות מהימנות לעובדים.

3. העברת מידע בין החברה ונותן השירותים

3.1. ככלל – העבודה תתבצע על גבי מערכות המידע של החברה ובלא הוצאת מידע ממערכות החברה לרשת נותן השירותים או לחזקתו.

3.2. העברת מידע ככל שתידרש במסגרת מתן השירות תתבצע באישור פרטני של מנהל אבטחת המידע של החברה, בהתאם לנהלי הוצאת המידע מהחברה.

3.3. לא תתבצע כל העברה של החומר למטרה כלשהי לכל גורם נוסף (חברת אם, שותפים עסקיים, קבלני משנה, וכו') למעט ביידוע וקבלת אישור ממנהל אבטחת המידע של החברה.

4. אבטחת מידע פיסית

4.1. נותן השירותים יפעיל אמצעים הולמים לבקרת הגישה הפיסית למשרדיו ומניעת חדירת גורמים בלתי מורשים.

4.2. מידור - נותן השירותים ינקוט באמצעים **הפיסיים** הנדרשים על מנת למנוע חשיפת עובדיו שאינם נמנים על "צוות כלל" או כל גורם אחר בעל גישה למשרדיו למידע של החברה, ובכלל זה:

4.2.1. הימנעות מהשארת מידע בתצורה של נייר או מדיות נתיקות (דיסקים וכדומה) ללא השגחה. מידע של החברה שאינו נמצא באותו רגע בטיפול של מי מחברי הצוות יישמר בכספת, ארון נעול או חדר נעול.

4.2.2. לרשות חברי "צוות כלל" יעמדו האמצעים הנדרשים על מנת להשמיד מידע בתצורות שלעיל עם תום השימוש בו – נייר ייגרס, ומדיות נתיקות יושמדו או יימחקו באופן מאובטח.

4.2.3. נותן השירותים ינקוט באמצעים הולמים (סימון בולט של פחי גריסה, פינוי חומר לגריסה וביצוע הגריסה בפועל בידי עובד מורשה, וכו') ויתדרך את עובדיו על מנת למנוע הגעה בשגגה של מידע רגיש לפחי אשפה וסלי ניירות במשרדים.

4.3. **הקשחת מערכות**

4.3.1. מערכות המחשב של נותן השירותים עליהן שמור או באמצעותן מעובד מידע של החברה תהיינה מאובטחות על פי הגדרות היצרן ועל פי הסטנדרטים המקובלים בשוק האבטחה.

4.3.2. המערכות תעודכנה באופן שוטף ותדיר בתיקוני ועדכוני אבטחה המופצים על ידי היצרנים.

4.4. **אבטחת מידע לוגית**

4.4.1. רשת נותן השירותים וכל מחשבי נותן השירותים יהיו מוגנים באמצעות מערכות אנטי וירוס המתעדכנות באופן שוטף בפני וירוסים ואיומים חדשים.

4.4.2. הקישור של רשת נותן השירותים לאינטרנט יהיה מאובטח באמצעות firewall ואמצעים נוספים על מנת למנוע הוצאת מידע מהרשת באמצעות שירותים שונים. במידה וישנם שירותים המאפשרים הוצאת וקבלת קבצים הם ייפתחו באופן מבוקר ומוגבל בלבד

4.4.3. יתבצע מעבר שוטף, על בסיס תקופתי, על הלוגים של מערכות האבטחה – לאיתור ניסיונות מוצלחים או כושלים להוצאת מידע באופן לא מורשה / מבוקר.

5. דיווח לחברה:

5.1. נותן השירותים יעדכן את החברה בכל חשש לדליפת מידע רגיש ממשרדי או ממערכות המחשב של נותן השירותים.

5.2. נותן השירותים יעדכן את החברה בנוגע לאירועי אבטחת מידע הנוגעים למידע של החברה המופקד בידי נותן השירותים ו/או המערכות בהן הוא שמור – בין אם להערכתו נגרם נזק ממשי ובין אם לאו.

5.3. נותן השירותים יעדכן את החברה במקרה של פיטורי עובדים על רקע של בעיות אמינות / מהימנות, או אירועים בתחום אבטחת המידע והביטחון, ובדגש אם עובדים אלה היו חשופים למידע של החברה.

6. ביקורות:

6.1. החברה שומרת לעצמה הזכות לערוך ביקורות (מעבר לאלה שתערוך חברת אבטחת המידע בה יבחר נותן השירותים), בחצרי או במערכות נותן השירותים לשם ווידוא עמידה בהנחיות הביטחון השונות. ביקורות אלו עשויות לכלול:

6.1.1. ביקור במתחם נותן השירותים. במסגרת ביקור זה יבדקו נושאים כגון:

6.1.1.1. תהליכי ונהלי עבודה רלוונטיים לעבודת נותן השירותים מול החברה.

6.1.1.2. יישום אמצעי הביטחון כפי שנדרשו על ידי החברה.

6.1.1.3. ראיונות עם חברי "צוות כלל".

ד"ר גיל שויד	24.2.2025
נותן השירותים	**תאריך**