קיט אבטחת מידע

SMS

הדרך הקלה לעבודה יעילה

אבטחת מידע

אנו בחברת SMS שמים בראש מעיינינו את נושא אבטחת המידע בחברה, החברה פועלת במגוון מישורים בכדי להבטיח את הסודיות והשמירה על מערכות המידע, טיפול במידע רגיש התנהלות בהתאם לרשימת הנהלים.

חברת SMS בעלת תו תקן ISO27001:2022 - מציגה עמידה מלאה בכל נהלי התקן ומוכיחה כי הארגון נוקט באמצעים המתאימים בכדי לממש את מחויבותו לשמירה על המידע ולנהלו בצורה יעילה. תהליך קבלת תו התקן מכיל מבדקים והתעדות המתבצעים מדי שנה.

אנו מציעים לחברות/ארגונים המבצעים עמנו שיתופי פעולה
מגוון ערוצים שמהם ניתן להתרשם ולקבל את תמונת המצב המלאה על החברה:

*לשאלות ולייעוץ מקצועי:

עו"ד אור לביא - מנכ"ל חברת PRIMESEC IT Regulations Solutions המלווה את חברת SMS בתחום אבטחת המידע.
עלות שעת התייעצות: ₪300

*טרום הבקשה להתייעצות יש למלא טופס הרשאה לחיוב לשעות עבודה.

יישום תקנות הגנת הפרטיות (אבטחת מידע) - חלק א'

סעיף בתקנות	נוסח הדרישה	מענה
2 (א)	(א) בעל מאגר מידע יגדיר במסמך הגדרות מאגר (להלן - מסמך הגדרות המאגר), את כל העניינים האלה לפחות : (1) תיאור כללי של פעולות האיסוף והשימוש במידע; (2) תיאור מטרות השימוש במידע; (3) סוגי המידע השונים הכלולים במאגר המידע, בשים לב לרשימת סוגי המידע שבפרט 3(1) בתוספת הראשונה ; (4) פרטים על העברת מאגר המידע, או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה, מטרת ההעברה, ארץ היעד, אופן ההעברה וזהות הנעבר; (5) פעולות עיבוד מידע באמצעות מחזיק; (6) הסיכונים העיקריים של פגיעה באבטחת המידע, ואופן ההתמודדות עמם; (7) שמו של מנהל מאגר המידע, של מחזיק המאגר ושל הממונה על אבטחת מידע בו, אם מונה כזה	מיושם
2 (ב)	(ב) בעל מאגר מידע יעדכן את מסמך הגדרות המאגר בכל עת שנעשה שינוי משמעותי בנושאים המפורטים בתקנת משנה (א), ויבחן את הצורך בעדכון כאמור, בשל שינויים טכנולוגיים ארגוניים או אירועי אבטחה כאמור בתקנה 11, בכל שנה עד 31 בדצמבר	מיושם
2 (ג)	(ג) בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר.	מיושם
3	חלה חובה למנות ממונה על אבטחת מידע, או מונה ממונה על אבטחת מידע במאגר המידע יחולו הוראות אלה : (1) ממונה אבטחה יהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחת הכפוף ישירות למנהל המאגר;	מיושם
3	(2) הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר;	מיושם
3	(3) הממונה יכין תכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, יבצע אותה ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו;	מיושם
3	(4) הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה;	מיושם
3	(5) הטיל בעל מאגר המידע על ממונה על אבטחה משימות נוספות על החובות המנויות בפסקאות (2) ו-(3), לשם ביצוע תקנות אלה, יגדירן בצורה ברורה;	מיושם
3	(6) בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו.	מיושם
4 (א)	(א) בעל מאגר המידע יקבע במסמך נוהל אבטחת מידע (להלן - נוהל האבטחה) בהתאם למסמך הגדרות המאגר ותקנות אלה, אשר יחייב כל בעל הרשאה בהתאם לפרטים מהנוהל שאליו הוא חשוף לפי תקנת משנה (ב).	מיושם
4 (ב)	(ב) בעל מאגר מידע ישמור את נוהל האבטחה כך שפרטים ממנו יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.	מיושם
4 (ה)	(ה) בעל מאגר מידע יבחן, אחת לשנה, את הצורך בעדכון הנוהל, ובלי לגרוע מן האמור, יבחן אם יש צורך בעדכונו של הנוהל במקרים אלה: (1) נעשים שינויים מהותיים במערכות המאגר או בתהליכי עיבוד מידע; (2) נודע על סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר.	מיושם
5 (ב)	(ב) המסמך המעודכן של מבנה מאגר המידע ורשימת המצאי יישמרו כך שפרטים מהם יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.	מיושם

יישום תקנות הגנת הפרטיות (אבטחת מידע) - חלק ב'

סעיף בתקנות	נוסח הדרישה	מענה
5 (ג)	(ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן - סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, ככל שהתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשר חודשים לפחות.	מיושם
5 (ד)	(ד) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערכו מבדקי חדירות למערכות המאגר לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים, אחת לשמונה עשר חודשים לפחות; בעל המאגר ידון בתוצאות מבדקי החדירות ויפעל לתיקון הליקויים שהתגלו, ככל שהתגלו.	מיושם
9 (ב)	(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה - (1) אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה;	מיושם
10 (ד)	נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.	מיושם
10 (ה)	(ה) בעל מאגר מידע יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר	מיושם
11 (ג)	(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית, יקיים בעל המאגר דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכונו של נוהל האבטחה; במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור אחת לרבעון לפחות.	מיושם
11 (ד)	(ד) אירע אירוע אבטחה חמור – (1) יודיע על כך בעל המאגר לרשם באופן מיידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע (2) רשאי הרשם להורות לבעל מאגר המידע, למעט לבעל מאגר מידע מן המנויים בסעיף 13(ה) לחוק, לאחר שנועץ בראש הרשות הלאומית להגנת הסייבר, להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע.	מיושם
12	בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, את הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה; בעל מאגר מידע המאפשר שימוש במידע מהמאגר בהתקן נייד או העתקה שלו להתקן נייד ינקוט אמצעי הגנה בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן נייד באותו מאגר מידע; לעניין זה יראו שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.	מיושם
14 (ג)	(ג) במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, ייעשה שימוש נוסף על אמצעי אבטחה כאמור בתקנות משנה (א) ו-(ב), באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה; לעניין גישה של בעל הרשאה למאגר מידע ברמת האבטחה הבינונית והגבוהה ייעשה שימוש באמצעי פיזי הנתון לשיטתו הבלעדית של בעל ההרשאה.	מיושם
18 (א)	(2) נהלים, להבטחת שחזור הנתונים כאמור בתקנה 17 (ב), ובלבד שביצוע השחזור יהיה באישור מנהל המאגר;	מיושם

המכון לבקרה ואיכות

תעודה

מס' I31577

הנני מאשר בזאת כי
מערכת ניהול אבטחת המידע של

אס.אמ.אס. סרביס מנג'מנט סיסטמס בע"מ
אלי הורוביץ 27, רחובות

נסקרה ונבחנה ע"י המכון לבקרה ואיכות ונמצאה מתאימה לדרישות התקן:

ISO/IEC 27001:2022

האישור תקף לפעולות הבאות:

ניהול אבטחת המידע במחלקת ה-IT הקשורה לפיתוח ויישום פתרונות טכנולוגיים מתקדמים בתחומי הביטוח, הפנסיה והפיננסים

בהתאם להצהרת הישימות מתאריך: 03.03.2025 גרסה: 2

אישור זה בתוקף עד:	**15.04.2028**
מחזור ההתעדה יסתיים בתאריך:	**15.04.2028**
מחזור התעדה קודם הסתיים בתאריך:	**NA**
תאריך אישור ועדת התעדה:	**15.04.2025**
תאריך אישור ראשוני:	**15.04.2025**

האישור מותנה בהמשך יישום מערכת ניהול,
בכפוף לביצוע מבדקי מעקב ע"י המכון לבקרה ואיכות

16.04.2025
תאריך

ניר הלפרן, מנכ"ל

המכון לבקרה ואיכות אי.קיו.סי בע"מ
רחוב שמירה אימבר גדיש 9, קריית אונו
טל': 03-9313555
דוא"ל: info@iqc.co.il, www.iqc.co.il

IAF MGMT. SYS. RvA C 560

המכון לבקרה ואיכות

מדיניות אבטחת מידע תקן ISO27001

- ✓ חברת "אס.אמ.אס סרביס מנג'מנט סיסטמס בע"מ" (להלן: "החברה") החליטה לאמץ את דרישות התקן הבינלאומי לניהול אבטחת מידע ת"י ISO 27001:2022 במטרה להיות המובילה בארץ בתחום פתרונות טכנולוגיים מתקדמים בתחומי הביטוח, הפנסיה והפיננסים, מתוך שאיפה למצוינות ברמת השירות, המקצועיות והידע ומתוך רצון לשמור ולהגן על המידע והידע של לקוחותיה ושלה.

- ✓ הנהלת החברה מקיימת מערכת לניהול אבטחת מידע (מנא"מ) כוללת, היוצרת מעטפת הגנה על המידע והידע, הליך של שיפור מתמיד וסביבת עבודה מקצועית ותומכת, תוך ראיה כוללת ששירות אמין, איכותי, מהימן ודיסקרטי ללקוח מהווה יסוד להצלחה ולעצם קיומה של החברה.

- ✓ הנהלת החברה רואה חשיבות רבה בהגנה על המידע בהיבטים של שלימות, זמינות ואמינות ורואה במערכת ניהול אבטחת המידע את המסגרת הניהולית להגנה על המידע. לצורך כך, הנהלת החברה תקצה את מירב המשאבים להבטיח את זמינות, שלמות ואמינות המידע ונכסי המידע המצויים ברשותה, ותנקוט באמצעים הולמים ומתאימים על מנת להגן על נכסי המידע של החברה ולקוחותיה מפני פגיעה, גניבה, שימוש בלתי הולם, שימוש לרעה וכל נזק אפשרי במטרה להבטיח את זמינותו, שלמותו ואמינותו.

- ✓ החברה תציב מטרות ויעדים ברי מדידה לשם יצירת הליך שיפור מתמיד של החברה ושל מערכת ניהול אבטחת המידע.

- ✓ החברה הגדירה מדיניות המשכיות עסקית לצורך הבטחת המשך פעילות החברה במקרה של אירוע אשר יפגע ביכולתה של החברה לספק שירות ללקוחותיה.

- ✓ הנהלת החברה תוודא את אמינותם ויושרם של בעלי התפקידים בחברה בהתאם לרמת רגישות התפקיד וסיווג המידע אשר ייחשף בפניהם ותגביל את הגישה למידע לבעלי התפקידים על פי הצורך התפעולי והתפקודי בלבד ובהתאם לעקרון "הצורך לדעת".

- ✓ עובדי החברה מודעים לחשיבות אבטחת המידע ומחויבים לשמירה על אבטחת המידע. הנהלת חברה תדאג לשמור על רמת המודעות הגבוהה של עובדיה באופן שוטף, תחתור ותשאף למצוינות ומקצועיות בכל תחומי פעילויותיה תוך קידום וטיפוח עובדיה, ועמידה לצידם בכל עת.

- ✓ הנהלת החברה מגדירה לנותני השירותים החיצוניים שלה דרישות בנושא אבטחת המידע ומוודאה קיום מודעות ועמידה בדרישות.

- ✓ החברה תאבטח ותסווג את המידע ונכסי המידע אשר מצויים ברשותה, בהתאם לנדרש בחוקים ותקנות, ועל פי העיקרון "המחמיר קובע".

- ✓ ההנהלה מחויבת לקיים במלואם את דרישות כלל החוקים, התקנות והתקנים המתייחסים לתחום אבטחת המידע בחברה בכל האתרים.

- ✓ החברה רואה בלקוח כשותף מלא להצלחתה ולקיומה, ותעשה את הכול על מנת לעמוד בציפיותיו, שביעות רצונו ובמוסכם איתו תוך מתן שירות מקצועי, אדיב ויצירתי.

- ✓ החברה, כחברה ישראלית, תתרום לצמיחת המשק הישראלי ולבניית חברה איכותית ומוסרית.

- ✓ החברה מצהירה בזאת כי אמינות, מהימנות ושירותיות, הינם מאבני היסוד לקיומה לאורך זמן.

יום רביעי י"ז אלול ה'תשפ"א 25/08/2021

יישום חובות מחזיק מאגרי מידע בהתאם לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017

1. **כללי:**

לקוחות חברת אס.אמ.אס סרביס מנג'מנט סיסטמס בע"מ (להלן: "**החברה**") מהווים הבעלים של מאגרי מידע הכוללים נתונים אודות לקוחותיהם. החברה, בהתאם לחוק הגנת הפרטיות, מהווה מחזיקה בחלק ו/או כלל מאגרי המידע הללו לצורך מתן שירותים ללקוחותיה.

לחברה קיימים גם מאגרי מידע אשר בבעלותה ורשומים ומעודכנים כחוק אצל רשם מאגרי המידע.

לחברה קיימת הסמכה לתקן ISO270001 (להלן: "**התקן**") משנת 2014.

הנחיית רשם מאגרי מידע בדבר תחולת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**התקנות**" או "**תקנות אבטחת מידע**") על ארגונים המוסמכים לתקן ISO/IEC 27001 (להלן: "**הנחיית הרשם**") קובעת כי גופים שקיבלו הסמכה לתקן ISO27001, ומקיימים את הוראותיו, לרבות את כל הבקרות הרלוונטיות המפורטות בנספח A לתקן, באופן בו הן מפורשות ומפורטות בתקן, יראו אותם כמי שמקיימים את הוראות התקנות במלואן ביחס למאגרים עליהם ניתנה הסמכה לתקן וכל עוד הסכמה עומדת בתוקפה ומילאו אחר כל הסעיפים המפורטים בהנחיה. נכון למועד בדיקתנו ההסמכה לתקן עומדת בתוקפה ועל כן חוות דעתנו מתייחסת להוראות התקנות בהן החברה מחוייבת לעמוד בהתאם להנחיית הרשם, תוך הנחה שהיא עומדת בהוראות התקן.

2. **פירוט אופן עמידת החברה בתקנות אבטחת מידע:**

תקנה 2- מסמך הגדרות מאגרי מידע

החברה רשמה את מאגרי המידע שלה כדין ברשות להגנת הפרטיות.

החברה הגדירה מסמך הגדרות מאגרי מידע המפרט את מאגרי המידע שבבעלותה, אשר כולל, בין היתר, את מטרות השימוש במאגרים, סוגי המידע שבמאגרים, מנהלי ומחזיקי המאגרים וכן את הסיכונים העיקריים של פגיעה באבטחת מידע ואופן ההתמודדות איתם ע"י החברה.

תקנה 3- ממונה אבטחה על המאגרים

החברה מינתה ממונה אבטחת מידע (להלן: "**הממונה**") הכפוף למנכ"ל החברה.

הממונה אחראי על כלל נושאי אבטחת המידע בחברה, לרבות הגדרת נהלים ותוכנית עבודה לבקרה שוטפת לעמידת החברה בתקנות אבטחת המידע ובבקרות התקן.

תקנה 4- נהלי אבטחת מידע

החברה הגדירה נהלים הכוללים את כל ההוראות המפורטות בתקנה 4 לתקנות אבטחת מידע ונושאים נוספים המכסים את הבקרות של תקן ISO27001.

הנהלים כוללים, בין היתר, מדיניות הסיסמאות של החברה, תהליך פתיחה/עדכון/סגירת משתמש, אופן הגישה מרחוק, תהליך מעקב אחר הלוגים של מנגנון הבקרה, ניהול מאובטח ומעודכן של מערכות מאגרי המידע, אבטחת תקשורת, ניהול טיפול וניהול אירועי אבטחת מידע, מדיניות גיבויים, פעילות החברה מול גורמי מיקור חוץ החל מתהליך בחירת הספק והגדרת דרישות אבטחת מידע, ניסוח הסכמי ההתקשרות מול הספק ופתיחת הרשאות גישה וכלה בסיום התקשרות עם הספק, הוראות לפיתוח מאובטח, כללי הצפנה, החזרת ציוד/מידע וסגירת ההרשאות.

החברה בוחנת את הצורך בעדכון נהלים אלה לכל הפחות אחת לשנה ו/או בעת שינויים מהותיים במערכות מאגרי המידע או בתהליכי עיבוד המידע, וכאשר נוצרים סיכונים טכנולוגיים חדשים הנוגעים למערכות מאגרי המידע.

תקנה 5- מיפוי מערכות מאגרי המידע וביצוע סקר סיכונים

החברה מחזיקה במסמך מעודכן של מבנה מאגרי המידע והמערכות בהתאם לדרישות התקנה.

החברה מבצעת סקרי סיכונים ומבדקי חדירה לפחות אחת לשנה בהתאם לתוכנית עבודה שוטפת וכאשר עולה צורך (כגון: שינוי מהותי במערכות החברה).

מבדקים אלה מבוצעים על ידי גופים חיצוניים המתמחים בתחום. תוצאות המבדקים נבחנות בקפידה, נידונות בישיבות הנהלה, ובמידת הצורך מבוצעות פעולות מתאימות לתיקון ליקויים.

תקנה 6- אבטחה פיזית וסביבתית

החברה הגדירה נוהל אבטחה פיזית, המפרט בין היתר, מפרט, בין היתר, הוראות בנושא אבטחת חדרי המחשוב וחדרים רגישים אחרים. זה זה מתעדכן לפחות אחת לשנה או בעת שינוי מהותי, כמתחייב בתקן.

הכניסה למשרדי החברה מבוצעת באופן מאובטח ומנוטר תוך הגבלת הגישה לשעות הפעילות בלבד.

שרתי המערכת מתארחים בחוות השרתים של בזק בינלאומי מתחת לפני האדמה. חוות השרתים עומדת בתקני אבטחה כמקובל בתחום כגון ISO27001, ISO9001, PCI DSS, TIER3+, ועוד.

תקנה 7- אבטחת מידע בניהול כוח אדם

החברה נוקטת באמצעים המקובלים בתהליכי מיון עובדים על מנת להבטיח, ככל שניתן, שהעובדים בחברה מתאימים לקבלת הגישה הנדרשת עבורם, תוך שימת דגש להתאמה בין רגישות המידע אליו נחשף העובד, היקף הרשאותיו וכישוריו.

החברה עורכת לעובדיה ומנהליה הדרכות מודעות לבעלי הרשאות גישה למידע המצוי במאגר המידע, בטרם מתן ההרשאות או בטרם שינוי ההרשאות הקיימות. ההדרכות עוסקות, ביו היתר, בחובותיהם לפי חוק הגנת הפרטיות, תקנות אבטחת המידע ונהלי אבטחת מידע של הספק. כל עובד חדש עובר הדרכה כאמור בסמוך למועד העסקתו. כמו כן, מתקיימות הדרכות תקופתיות לכלל העובדים לפחות אחת לחצי שנה.

בנוסף, החברה מקיימת ביקורות "שולחן נקי" תקופתיות לכלל עובדי החברה.

<u>תקנה 8- ניהול הרשאות גישה</u>

החברה הגדירה נהלים להקצאת הרשאות, בקרת רשומות ובקרת תיעוד. הקמת משתמש חדש ופתיחת חשבון תתאפשר רק לעובדים אשר נקלטו, סיימו את תהליך הקליטה וחתמו על כל ההצהרות וההתחייבויות שלהם, לרבות השתתפות בהדרכת מודעות.
הקצאת הרשאות מבוססת על עקרון הצורך לדעת בלבד. החברה מנהלת רישום ותיעוד של בעלי ההרשאה ומקיימת בקרת הרשאות לפחות אחת לשנה.

<u>תקנה 9- זיהוי ואימות</u>

החברה הגדירה בנוהל מדיניות סיסמאות מורכבת ומחמירה עבור בעלי ההרשאות מטעמה. הנוהל קובע, בין היתר, את חוזק הסיסמה הנדרשת, מספר הניסיונות השגויים טרם נעילת חשבון, תדירות החלפת סיסמאות, ניתוק אוטומטי לאחר פרק זמן של אי פעילות ואופן טיפול בתקלות הקשורות באימות זהות. הסיסמאות מוצפנות בהצפנה חד כיוונית בבסיס הנתונים.

קיים תהליך מסודר לסיום העסקת עובד הכולל סגירת הרשאות באופן מידי.

<u>תקנה 10- בקרת קוד גישה (מנגנון בקרה)</u>

קיים מנגנון בקרה אוטומטי אשר מאפשר ביקורת על הגישה למערכות המאגר (להלן: "**מנגנון הבקרה**") ומפיק את הלוגים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה. הלוגים של מנגנון הבקרה נשמרים באופן מאובטח לפחות למשך 24 חודשים. גישה לניהול מנגנון הבקרה קיימת למנהל הפיתוח וה- CTO בלבד. העובדים מיודעים אודות מנגנון הבקרה וניטור פעולותיהם במחשבי החברה.

<u>תקנה 11- אירועי אבטחת מידע</u>

מתקיים דיונים תקופתיים לפחות אחת לרבעון בנושא אבטחת מידע ולפחות אחת לשנה הדיון מתקיים בהשתתפות הנהלת החברה.

החברה הגדירה נוהל עבודה ייעודי לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים הנדרשים וכן הוראות לעניין דיווח ללקוח על אירועי אבטחה ועל הפעולות שננקטו בעקבותיהם.

החברה בוחנת אחת לשנה את הצורך בעדכון נוהל המשכיות עסקית ונוהל אירוע חריג, לאור אירועי אבטחת מידע. החברה הגדירה תהליך מסודר לעניין דיווח על אירועים לרשם מאגרי המידע ולבעלי עניין נוספים בהתאם לצורך.

<u>תקנה 12- התקנים ניידים</u>

החברה הגבילה את האפשרות לחיבור התקנים ניידים ונוקטת באמצעי הגנה.

<u>תקנה 13- ניהול מאובטח ומעודכן של מערכות המאגר</u>

החברה מקפידה על התקנת תוכנת הגנה תקנית ומעודכנת נגד נוזקות על מחשבים המכילים מידע השייך ל לקוחותיה.

החברה מיישמת הפרדה לוגית אפליקטיבית בין בסיס הנתונים של הלקוחות השונים, תוך שילוב הגנות על בסיס הנתונים עפ"י הוראות תקן ISO 27001:2022 ולפי פרקטיקה מקובלת .מתקיים ניטור שינויים בבסיסי הנתונים.

החברה מקפידה על שימוש במערכות הפעלה, דפדפנים, בסיסי נתונים ותשתיות תוכנה בגרסאות נתמכות בלבד. לא נעשה שימוש במערכות EOL.

<u>תקנה 14- אבטחת תקשורת</u>

החברה מיישמת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק למחשב, לרבות Firewall והפעלת מודולים רלוונטיים (כגון: IPS) ומערכת הגנה מנוהלת לכלל תחנות העבודה והשרתים.

גישה מרחוק מבוצעות באמצעות Forti Client וכתובת IP קבועה של החברה מרשת החברה ומכשיר סלולרי מוגדר (כתובות IP שהוגדרו מבעוד מועד).

<u>תקנה 15- מיקור חוץ</u>

תקנות אבטחת מידע קובעות כי תקנה זו אינה חלה על מחזיק המאגר.

נציין כי החברה נותנת שירותי מיקור חוץ ללקוחותיה ומתחייבת לסייע ולהוות שלוחה של כל לקוח ליישום התקנה במלואה לרבות, שמירת סודיות המידע, הגבלת גישה לגורמים מורשים בלבד, מחיקת המידע בסיום התקשרות ו/או לפי הוראות כל דין, שימוש במידע לצורך ביצוע שירותים בלבד ובכפוף להסכם שירות.

בעת התקשרות עם ספקי משנה החברה מחתימה אותם על התחייבויות לשמירת סודיות ואבטחת מידע התואמות באופן מהותי את התחייבויות החברה כמפורט בתקנות אבטחת מידע.

<u>תקנה 16- ביקורת תקופתית</u>

בהתאם להנחיית הרשם, החברה פטורה מקיום תקנה זו. יחד עם זאת, החברה מלווה על ידי חברת אבטחת מידע חיצונית ליישום הדרישות לעמידה בתקנות אבטחת מידע ובתקן, כן מבוקרת על ידי גוף התעדה חיצוני לעמידה בתקן.

<u>תקנה 17- שמירת נתוני אבטחה</u>

החברה הגדירה נוהל סדור לשמירה וגיבוי נתוניה ובתוכם: נתוני בקרה ותיעוד של מנגנון הבקרה, רשימת הרשאות מעודכנת, תוצרי ניטור ותיעוד של אירועי אבטחת מידע, תוצרי בקרה ופיקוח ש החברה על פעילות פנים ארגונית (סקרי סיכונים, מבדקי חדירה, הדרכות, תרגילים, תחקירים ועוד) ופעילות ספקיה, דו"חות ביקורת אבטחת מידע וכיו"ב.

<u>תקנה 18- גיבויים ושחזורים</u>

החברה הגדירה נוהל לביצוע גיבויים ושחזורים ושומרת את הגיבויים באופן מאובטח למשך 24 חודשים לפחות. החברה מבצעת בדיקות שחזור יזומות באופן תקופתי לגיבויים.

הסכם הגנת פרטיות ואבטחת מידע

שנחתם ביום _____ לחודש _____ בשנת _____

בהמשך לטופס ההצטרפות ורשימת השירותים שבו (להלן: "**טופס ההצטרפות**"), שנחתם בין אס.אמ.אס סרביס מנג'מנט סיסטמס בע"מ (להלן: "**הספק**") לבין _____ (להלן: "**הלקוח**") ולאור הוראות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**תקנות אבטחת מידע**") הצדדים מעוניינים להוסיף את התנאים הבאים להתקשרותם:

הוראות כלליות:

1. הסכם זה הוגדר ונחתם מראש על ידי הספק.

2. הלקוח מתבקש להחזיר את ההסכם חתום לספק, לאחר שמילא את בעלי ההרשאות מטעמו בנספח א' להסכם.

3. הספק והלקוח מתחייבים לפעול על פי כל דין, לרבות הוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן: החוק" או "חוק הגנת הפרטיות") התקנות שהותקנו לפיו, הנחיות רשם מאגרי המידע והרשות להגנת הפרטיות, הנחיות רשות שוק ההון, ביטוח וחיסכון וכיוצא בזאת, ולפי הוראות שיתקבלו מעת לעת על ידי הלקוח.

4. הלקוח יוגדר "בעל מאגר מידע" והספק יוגדר "מחזיק במאגר מידע", כהגדרתם בחוק הגנת הפרטיות.

5. הלקוח מצהיר כי שמו ומספר זהותו הם כמפורט בטופס ההצטרפות, וכי הוא הבעלים הרשום והיחיד של מאגר המידע. כן מתחייב הלקוח, כי בכל תקופת הסכם זה יהיה המאגר רשום כחוק.

6. הספק רואה חשיבות רבה בהגנת פרטיות המידע ואבטחתו ומשקיע משאבים רבים להגנה על המידע. על כן, בנוסף לחוק והוראותיו, הספק מקיים מערכת ניהול אבטחת מידע בהתאם לדרישות תקן ISO 27001: 2022 החל משנת 2014, הנבחנת ונסקרת לפחות אחת לשנה על ידי חברת ייעוץ וגוף התעדה חיצוני.

7. הספק מצהיר כי לשם מתן השירותים אשר פורטו בטופס ההצטרפות אין לו גישה למערכות המידע של הלקוח. לספק ולבעלי ההרשאות מטעמו גישה למידע שהלקוח מזין במערכות הספק בלבד.

8. בעלי ההרשאות מטעם הלקוח לנתונים המוחזקים על ידי הספק מפורטים בנספח א' להסכם זה ולא תותר כל הוספה ו/או שינוי של בעלי ההרשאות מטעם הלקוח אלא בהודעה מראש ובכתב אל הספק, הכוללת ציון שם, מספר תעודת זהות, ותפקיד.

9. בעלי ההרשאות מטעם הספק – לחץ כאן. קישור זה יעודכן בכל שינוי בבעלי ההרשאות, ככל שיהיה, ולפחות אחת לשנה.

10. במסגרת מתן השירותים כפי שהוגדרו בטופס ההצטרפות, הספק רשאי לעבד רק את סוגי המידע הבאים:

    10.1. כל מידע שהלקוח מזין במערכות הספק על הלקוח ו/או על לקוחות של הלקוח.

    10.2. מידע על הלקוח עשוי לכלול, בין היתר: זיהוי לקוח ופרטי קשר (שם, כתובת, תפקיד, פרטי יצירת קשר, שם משתמש); מידע פיננסי (פרטי כרטיס אשראי, פרטי חשבון בנק, פרטי תשלום).

    10.3. מידע על לקוחות קצה (מבוטחים / עמיתים) של הלקוח עשוי לכלול, בין היתר: פרטי זיהוי ופרטי קשר שם, תאריך לידה, מין, מקצוע או נתון דמוגרפי אחר, כתובת, תפקיד, פרטי יצירת קשר לרבות כתובת דוא"ל; קשרים משפחתיים ופרטי מוטבים; מידע כלכלי (נכסים, חובות, פרטי חסכונות פנסיוניים, פרטי קופות גמל, חשבון בנק לתשלום); נתוני ביטוח; נתוני חיסכון; מידע בריאותי; נתוני "מסלקה" ו "הר הביטוח"; מידע טכנולוגי (כתובת IP, נתוני שימוש, עוגיות, נתוני ניווט מקוונים, נתוני מיקום, נתוני דפדפן). וזאת למטרת ביצוע השירותים בלבד, כפי שהוגדרה בטופס ההצטרפות.

11. העברת מידע בין הלקוח לספק תתבצע באמצעות הזנת המידע על ידי הלקוח במערכות הספק.

12. הספק לא יעביר וכן לא יאפשר גישה ו/או הרשאות צפייה ו/או הרשאות עיבוד כלשהן לגבי המידע המפורט בסעיף 10 לאף גורם מבלי שקיבל את אישור הלקוח מראש ובכתב. לשם כך, ולצורך ביצוע השירותים המפורטים בטופס ההצטרפות בלבד, הלקוח מאשר לספק להתקשר עם ספקי משנה לצרכים הבאים:

12.1. ספקי אחסון, תפעול ותחזוקת השרתים (בזק בינלאומי).

12.2. ספקי פיתוח.

12.3. ספקי שירות.

12.4. ספקי תמיכה.

13. הספק מצהיר בזאת כי בעת התקשרות עם ספק משנה כאמור בסעיף 21, יחתים הספק את ספקי המשנה על התחייבויות לשמירת סודיות ואבטחת מידע התואמות באופן מהותי את התחייבויות החברה כמפורט בהסכם זה ובתקנות אבטחת מידע.

14. הלקוח יהיה רשאי, בתדירות שלא תעלה על אחת ל- 12חודשים, אלא אם אירע אירוע אבטחת מידע אצל הספק הקשור למידע של הלקוח ו/או קיימות הפרות של הספק את חובותיו בהתאם למסמך זה, בתיאום זמן סביר מראש עם הספק, לבצע ביקורות על קיום התחייבויות הספק על פי הסכם זה והוראות הדין החלות על הספק, בכפוף לאמור להלן: (א) הביקורת ת יערך בשעות העבודה המקובלות וללא הפרעה ככל הניתן לפעילות השוטפת של הספק. (ב) הביקורת לא תכלול גישה לשרתי ומערכות הספק. (ג) לא יתאפשר לגורם המבקר לגשת או לצפות במידע של לקוחות אחרים או לערוך ביקורת אצל צדדים שלישיים זולת הספק עצמו. (ד) הגורם המבקר יחתום על הסכם סודיות אישי כלפי הספק, בנוסח המקובל על הספק. (ה) ממצאי דוח הביקורת יחשבו כמידע סודי של הספק. (ו) בכפוף לתשלום לפי שעות העבודה שיידרשו מהספק להקצות לטובת הביקורת.

15. הספק מתחייב להעביר דיווח מידי בכל מקרה של דליפת המידע מהמאגר או שימוש חורג מההרשאה שניתנה לספק ו/או למי מטעמו.

16. הספק מתחייב לדווח ללקוחותיו על פי דרישה, אחת לשנה, אודות אופן ביצוע חובותיו בהתאם לתקנות אבטחת מידע.

17. כל הודעה לפי הסכם זה בקשר למאגר ו/או לגישה אל נתוני המאגר ו/או לשינוי מורשים מטעם הלקוח, תועבר בכתב (לרבות בדוא"ל) אל ממונה אבטחת המידע של הספק (כמפורט מטה) או אל איש הקשר שצוין בטופס ההצטרפות, לפי העניין.

<u>סודיות:</u>

18. "מידע", במסמך זה: כל חומר, מסמך ו/או מידע אחר הנוגע לפעילות הלקוח ו/או חבריו ו/או לקוחותיו ו/או עובדי ו ו/או עסקיו אשר אינו נחלת כלל הציבור (למעט אם הפך לכזה בשל מעשה/מחדל של הספק) לרבות, מבלי לגרוע מכלליות האמור לעיל, מידע אודות משאבי הלקוח; מידע בדבר סודות מסחריים ו/או מקצועיים, הזמנות והסכמים מכל סוג ו/או מידע המוגן מכוח חוק הגנת הפרטיות ו/או בהתאם לכל דין אחר החל או עשוי לחול על הלקוח.

19. ידוע לספק כי לצורך מתן השירותים ללקוח, תהא לו גישה למידע כהגדרתו לעיל. כמו כן, ידועה וברורה לספק רגישותו המיוחדת של המידע והצורך בשמירה קפדנית על חסיונו ועל הנזק הכבד שעשוי להיגרם עקב חשיפתו על ידי או עשיית שימוש בו על כל המשתמע מכך.

20. הספק מתחייב לשמור בסודיות מוחלטת כל מידע אשר יגיע אליו מתוקף מתן השירותים ללקוח או בדרך אחרת. הספק מתחייב שלא להחזיק ברשותו ולא לעשות כל שימוש, בכל מידע באשר הוא שלא לצורכי ביצוע השירותים המפורטים בטופס ההצטרפות. הספק מתחייב שלא לגלות מידע כזה או חלקו, במישרין או בעקיפין, לכל אדם או גוף, אלא לצורך ביצוע השירותים לפי ההסכם ובכפוף להסכמת הלקוח. למעט:

20.1. העברת מידע מוגבלת לעובדים (לרבות נותני שירות מטעם הספק) אשר להם צורך של ממש בקבלת המידע לצורך ביצוע השירותים בלבד, ובלבד שהובהר לעובדים אלה כי מדובר במידע סודי, והם חתומים כלפי הספק על כתב סודיות בנוסח דומה לכתב סודיות זה.

20.2. על פי דרישת ערכאה מוסמכת או רשות שלטונית מוסמכת על פי דין, ובלבד שהספק יודיע ללקוח באופן מידי על קבלת דרישה למסירת המידע (ככל שלא קיימת מניעה על פי דין למתן הודעה כאמור), ויאפשר ללקוח, ככל שהדבר בידי הספק, להתגונן בפני כל דרישה כאמור והספק ימסור רק את אותו חלק של המידע הסודי ו/או המידע החסוי שנדרש במפורש למסור.

21. הספק מתחייב לפעול כך שנתונים ומידע אשר יועברו אליו בהתאם להסכם זה, יאובטחו כך שלא תתאפשר גישה, בין באופן אקטיבי ובין באופן פאסיבי, למידע ולנתונים אלו, לאיש מלבד המורשים לכך החתומים על כתב התחייבות לשמירת סודיות כלפי הלקוח.

22. לא להעתיק ו/או להרשות לאחרים ו/או לגרום לאחר לבצע במידע – שכפול, העתקה, צילום, תדפיס וכל צורת העתקה אחרת שלא למטרת ביצוע עבודתי.

23. על העותקים של המידע יחולו הוראות התחייבות זו וכל האמור לגבי המידע יחול גם על עותקיו.

24. לשמור בהקפדה את המידע שיימסר לרשות הספק ולמנוע אובדנו ו/או הגעתו לידי אחר.

25. לא לעשות כל שימוש במידע בין בעצמו ובין באמצעות אחרים ולא להעביר ו/או למסור כל מידע לצד שלישי

לכל מטרה ומכל סיבה שהיא.

26. למען הסר ספק, מוצהר ומוסכם כי אין בעצם גילוי המידע על ידי הלקוח והעברתו אל הספק כדי להעניק לו כל

זכות במידע.

27. התחייבויות הספק דלעיל תחולנה עלי ו אישית וכן על כל תאגיד ו/או גוף ש יקים ו/או שיהיה שותף בו, ו/או בעל שליטה בו, בין כבעל מניות, ובין בכל דרך אחרת, בין במישרין ובין בעקיפין, וכן על כל עובד מטעמו שייתן השירות.

28. תוקפה של התחייבות זו אינו מוגבל בזמן.

29. התחייבות זו לא תחול על מידע אשר התקבל מהלקוח ואשר הספק יוכיח לגביו בכתובים כי:

29.1. המידע היה ידוע לספק לפני קבלת המידע מהלקוח.

29.2. המידע היה ידוע ברבים או שהיה ניתן להשגה על ידי הציבור הרחב לפני יום העברתו לספק.

29.3. המידע הפך למידע ציבורי או ניתן להשגה על ידי הציבור לאחר מועד העברת המידע על ידי הלקוח לספק בלא שהיה הספק אחראי או מעורב בתהליך.

29.4. המידע הגיע לספק בדרך חוקית של רכישת זכויות או בכל דרך חוקית שהיא.

<u>דרישות אבטחת מידע:</u>

30. הנחיות כללית:

30.1. הספק מינה ממונה על אבטחת המידע (להלן: "הממונה") בהתאם לסעיף 17ב לחוק הגנת הפרטיות ולתקנה 3 לתקנות אבטחת מידע. הממונה בעל הכשרה מתאימה וכפוף למנכ"ל הספק.

30.2. הספק הגדיר נהלי אבטחת מידע, כמפורט בתקנה 4 לתקנות אבטחת המידע ובהתאם לתקן ISO 27001:2022. הנהלים מבוקרים ונסקרים לכל הפחות אחת לשנה.

30.3. הספק הגדיר מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, הכל בהתאם למפורט בתקנה 5 לתקנות אבטחת המידע.

30.4. הספק יוזם ביצוע סקרי סיכונים ומבדקי חדירה למוצר שלו אחת לשנה לפחות ע"י חברה חיצונית.

31. <u>אבטחה פיסית וסביבתית – תקנה 6 לתקנות אבטחת מידע:</u>

31.1. הספק שומר את מאגרי המידע וכן את התשתיות והמערכות המשמשות את המאגרים, בחוות השרתים של בזק בינלאומי העומדת בתקני אבטחה כמקובל בתחום, כגון , ISO27001, ISO9001, PCI DSS TIER3+, ועוד.

32. <u>אבטחת מידע בניהול כוח אדם – תקנה 7 לתקנות אבטחת מידע:</u>

32.1. הספק מחתים את בעלי ההרשאות מטעמו על הצהרות סודיות הכוללות, בין היתר, התחייבות לשמירה מוחלטת על סודיות המידע של הלקוח, שימוש במידע רק בהתאם לאמור בהסכם ההתקשרות בין הספק ללקוח ויישום אמצעי האבטחה הקבועים בהסכם זה.

32.2. הספק מקצה ומשנה הרשאות גישה למידע המצוי במאגר המידע רק לאחר נקיטת אמצעים סבירים, המקובלים בהליכי מיון ושיבוץ עובדים.

32.3. הספק מקיים הדרכות מודעות לבעלי הרשאות גישה למידע המצוי במאגר המידע, בטרם מתן ההרשאות או בטרם שינוי ההרשאות הקיימות. ההדרכות עוסקות, בין היתר, בחובותיהם לפי חוק הגנת הפרטיות, תקנות אבטחת המידע ונהלי אבטחת מידע של הספק. כל עובד חדש עובר הדרכה כאמור בסמוך למועד העסקתו. כמו כן, מתקיימות הדרכות תקופתיות לכלל העובדים לפחות אחת לחצי שנה.

33. <u>הזדהות וניהול הרשאות – תקנות 8-9 לתקנות אבטחת מידע:</u>

33.1. כחלק מתהליך קליטת עובד חדש בחברה/שינוי הרשאה, באחריות מנכ"ל או מי שמונה על ידו להקצות לעובד הרשאות גישה למערכות המידע בהתאם לתפקיד המיועד ולרגישות המידע. הקמת משתמש חדש ופתיחת חשבון תתאפשר רק לעובדים אשר נקלטו, סיימו את תהליך הקליטה וחתמו על כל ההצהרות וההתחייבויות שלהם, לרבות השתתפות בהדרכת מודעות.

33.2. הספק הגדיר לבעלי ההרשאות מטעמו מדיניות סיסמאות מורכבת ומחמירה.

33.3. הסיסמאות מוצפנות בהצפנה חד כיוונית בבסיס הנתונים.

33.4. הספק הגדיר את אופן טיפול בתקלות הקשורות באימות זהות.

33.5. הספק הגדיר תהליך 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.

33.6. הקמה, הגדרה ועדכון משתמש ללקוחות החברה:

32.6.1. כל לקוח מורשה לפתוח לעצמו חשבון משתמש ריק (ללא ממשקים). ללקוח תהיה גישה לסביבה שלו בלבד.

33.6.2. לקוח שעבר את כל ההדרכות וחתם על כל המסמכים הדרושים (הסכם התקשרות, סודיות ודרישות אבטחת מידע יקבל את ההרשאות בהתאם למוגדר בהסכם ההתקשרות.

34. <u>בקרה ותיעוד גישה – תקנה 10 לתקנות אבטחת מידע:</u>

34.1. הספק מתעד בלוג את השדות הבאים:

- זיהוי ואימות
- נעילת משתמש
- פעולות עדכון ע"י המשתמשים כולל שמירת ערך קודם
- העלאת תכנים
- גישה מרחוק
- תיעוד כל מקרה שבו התגלה אירוע אבטחת מידע מבוסס התיעוד על רישום אוטומטי

34.2. הספק שומר את הלוגים הנ"ל באופן מאובטח, למשך 24 חודשים, לכל הפחות.

34.3. הספק הגדיר נוהל בדיקה שגרתי של הלוגים למנגנון הבקרה כולל דו"ח של הבעיות שהתגלו והצעדים שננקטו בעקבותיהן.

35. <u>אירועי אבטחת מידע – תקנה 11 לתקנות אבטחת מידע:</u>

35.1. הספק הגדיר הוראות בנוהל האבטחה שלו לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים הנדרשים וכן הוראות לעניין דיווח ללקוח על אירועי אבטחה ועל הפעולות שננקטו בעקבותיהם.

35.2. הספק ידווח גם לרשם מאגרי מידע אודות אירוע אבטחה חמור וישמור את התיעוד באופן מאובטח, למשך 24 חודשים לכל הפחות.

35.3. הספק מקיים דיונים באירועי האבטחה לפחות אחת לרבעון ובוחן את הצורך בעדכון נהלי האבטחה שלו.

36. <u>ניהול מאובטח ומעודכן – תקנות 12-13 לתקנות אבטחת מידע:</u>

36.1. הספק הגביל את האפשרות לחיבור התקנים ניידים ונוקט אמצעי הגנה בנדון.

36.2. הספק התקין תוכנת הגנה תקנית ומעודכנת נגד נוזקות על מחשבים המכילים מידע השייך ללקוח.

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

36.4. הספק מבצע הפרדה לוגית - אפליקטיבית בין הנתונים של הלקוח לבין נתונים של לקוחות אחרים.

36.5. הספק מיישם הגנות על בסיס הנתונים עפ"י הוראות תקן ISO 27001:2022 ולפי פרקטיקה מקובלת.

36.6. הספק מוודא ניטור שינויים בבסיסי הנתונים.

36.7. זמינות מרבית – הספק ידווח ללקוח על כל השבתה של המערכת.

36.8. הספק ישמור את המידע כל עוד נמשך השירות ועד 30 ימים ממועד סיום ההתקשרות.

36.9. הספק עושה שימוש במערכות הפעלה, דפדפנים, בסיסי נתונים ותשתיות תוכנה בגרסאות נתמכות בלבד. לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים.

37. <u>אבטחת תקשורת – תקנה 14 לתקנות אבטחת מידע:</u>

37.1. הספק נוקט באמצעי אבטחה הולמים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת או אל קווי התקשורת בין הלקוח אל הספק (לכל הפחות - WAFוFirewall, הצפנה בפרוטוקול נתמכים בלבד).

37.2. הספק התקין אמצעי הגנה מתאימים לחיבור לרשת האינטרנט או לרשת ציבורית אחרת מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש.

37.3. גישה מרחוק לעובדי החברה לרשת ו/או מערכות החברה תתבצע מכתובת IP קבועה בלבד שתוגדר ברכיב ה- FW ובאישור מנהל אבטחת מידע.

37.4. הלקוח יכול לבחור שהגישה שלו תהיה דרך כתובת IP קבועה.

38. <u>גיבויים ושחזורים:</u>

38.1. הספק הגדיר נוהל לביצוע גיבויים ושחזורים של נתוני האבטחה, בהתאם לתקנות 17 ו-18 לתקנות אבטחת מידע.

39. <u>דרישות נוספות - פעילות בענן</u>:

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

39.2. הספק עושה שימוש בגרסאות דפדפנים נתמכות.

39.3. הספק הגדיר ממשק ניהול בגישה מהרשת בלבד או מכתובות שיסופקו על ידה.

ולראיה באו הצדדים על החתום:

_____	_____
הספק	**הלקוח**

אס.אמ.אס בע"מ
סרביס מנג'מנט סיסטמס
514411974

נספח א' - רשימת בעלי הרשאה מטעם הלקוח)בעל המאגר(

	שם מלא	מספר ת.ז.	תפקיד אצל הבעלים	דוא"ל
.1	_____	_____	_____	_____
.2	_____	_____	_____	_____
.3	_____	_____	_____	_____