משקי דרום

מערכות מידע

טיוטת דוח ביקורת | 31 ביולי 2025

31 ביולי 2025

לכבוד

ועדת הביקורת

<u>משקי דרום אחזקות</u>

א.ג.נ.,

הנדון: <u>דוח ביקורת בנושא מערכות מידע</u>

בהתאם לתוכנית הביקורת הפנימית לשנת 2025 של משקי דרום אחזקות , ערכנו ביקורת בנושא מערכות מידע.

נציין, כי דוח ביקורת מתאפיין בהבלטת הליקויים. אין בכך בכדי להעיב על נושאים שנמצאו תקינים ועבודתם המסורה של העוסקים בנושא.

טיוטת דוח הביקורת הועברה למנכ"ל משקי הדרום, אחראי מחשוב ומנהלת מטה ומשאבי אנוש. ביום 22 ביוני 2025, תגובתם התקבלה ביום 30 ביולי 2025 ומצורפת לדוח בסעיפים הרלוואנטיים.

רצ"ב הדוח שבנדון.

אנו עומדים לרשותכם בכל שאלה ועניין.

בכבוד רב,

זיו האפט יעוץ וניהול בע"מ

BDO Israel, an Israeli partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms

רקע כללי

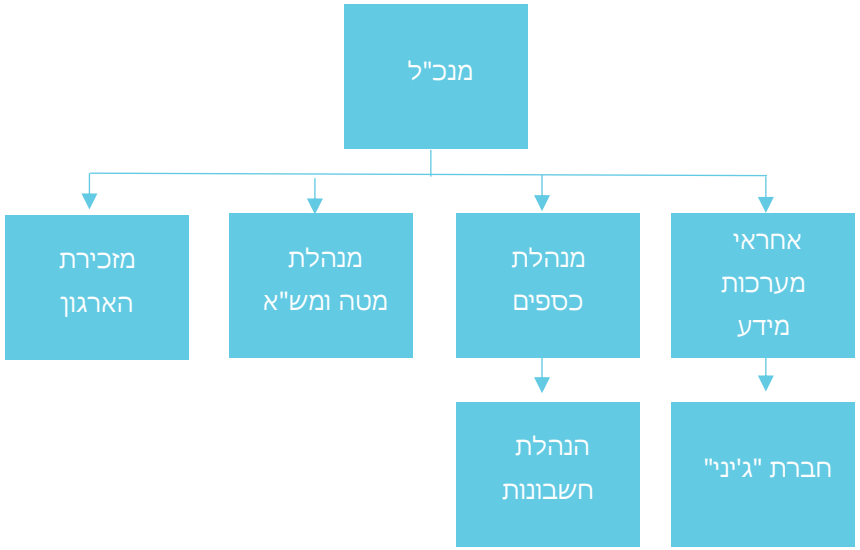
ארגון משקי דרום מנהל פעילויות שונות הכרוכות בהיבטי מערכות מידע, ביניהן מערכות המידע של הקיבוצים, ספקים, הנהלת החשבונות, ועוד.

בעידן הנוכחי של הקדמה הטכנולוגית, מערכות המידע הממוחשבות מהוות חלק בלתי נפרד מפעילויות הארגון. פגיעה בחיסיון המידע, בשלמותו או בשרידותו עלולה לגרום נזק לארגון וגם לגורמים שפרטיהם כלולים במאגרי המידע שלו, ולפיכך חלים על הארגון חוקים ותקנות הנוגעים לאבטחת המידע. בהם חוק הגנת הפרטיות התשמ"א-1981 ("להלן: "החוק") ותקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017 (להלן: "התקנות"), חוק המחשבים התשנ"ה - 1995 ועוד.

סיכוני סייבר עלולים להתממש כתוצאה מניצול של חולשות במערכות, תהליכים וגורם אנושי עד כדי שיבוש הפעילות השוטפת, למנוע מהארגון אספקת שירותים ללקוחות הארגון ולחברות השונות הנמצאות תחת שליטת ואחריות הארגון ואף לחשוף את הארגון לתביעות משפטיות ועיצומים רגולטוריים ועוד.

בשנים האחרונות גדל היקף תקיפות הסייבר באמצעים ובטכניקות שונים. בשל כך נוצר הצורך באבטחת מידע הבאה להגן על שלמות המידע מפני חשיפה, שימוש או העתקה, על ידי גורמים שאינם מורשים. בארגון קיימים מספר מאגרי מידע (כפי שיפורט בהמשך), הנדרשים לרמת אבטחה בינונית כמוגדר בחוק ובתקנות.

להלן תרשים ארגוני של העוסקים במערכות מידע בארגון:



אחראי מערכות מידע - משמש כנציג הארגון מול חברת המחשוב, חברת "ג'יני".

חברת "ג'יני" – באחריות תחזוקת מערכת המחשוב והתשתיות. לרבות שירותי IP, טיפול בשרתים ומחשבי קצה, קשר בין חברות התוכנה לארגון, טיפול שוטף בתקלות ועדכוני תוכנה. לא קיימת יחידת מחשוב ייעודית, בארגון.

מזכירת הארגון – אחראית על רישום צרכי הארגון / העובדים ותאום מול נציג חברת "ג'יני" המגיע לארגון יום אחד בשבוע.

צוות מחשוב – באחריות הצוות לקבוע מדיניות בנושאי מערכת המחשוב, כמפורט בהמשך.

רות, היקף ושיטת הביקורת

1. מטרת הביקורת

בהתאם לתוכנית הביקורת הפנימית לשנת 2025, ערכנו ביקורת בנושא מערכות מידע.

מטרות הביקורת :

- מיפוי ותחום מערכות מידע רלוונטיות.
- בחינת נהלים רלוונטיים למערכות המידע, יישום הפרדת תפקידים נאותה בסביבת מערכות אלו וקיום תהליכי הערכת סיכונים.
- בחינת עמידה בחוק שמירת מאגרי מידע וחוק הגנת הפרטיות.
- גישה לוגית למערכות המידע- סיסמאות למערכות, ניהול ההרשאות במערכות המידע לרבות תהליך מתן הרשאות וסגירתן.
- גישה פיזית- למערכות המידע, השרתים, ניהול ובקרה לכניסה לשרתים.
- ניהול מערכות המחשוב מול ספקי מערכות המידע.
- ניהול תשתית המערכת, הגיבויים ומשאבי המחשוב הנדרשים עבורה, לרבות התאוששות במקרה של קריסה.
- בחינת דוחות הבקרה המופקים מהמערכת.
- בדיקת תהליכי ניטור, ממשקים במערכת כולל נתיבי ביקורת, דוחות בקרה וציות לנהלים.

במסגרת הביקורת ערכנו בדיקה של תהליכי העבודה בהתייחס לשנים 2024 – 2022.

2. שיטת העבודה

ערכנו שיחות עם אחראי מערכות מחשוב, מנהלת מטה ומשאבי אנוש, מזכירת הארגון, חשבת הארגון, נציג חברת ""ג'יני" האחראי על מתן השרות למשקי דרום בחברת "ג'יני".

כמו כן, אספנו וסקרנו מסמכים רלוונטיים, ביצענו בדיקות שונות וניתחנו את הנתונים.

טיוטת דוח הביקורת הועברה למנכ"ל משקי הדרום, אחראי מחשוב ומנהלת מטה ומשאבי אנוש. ביום 22 ביוני 2025, תגובתם התקבלה ביום 30 ביולי 2025 ומצורפת לדוח בסעיפים הרלוואנטיים.

אנו מודים לכולם על שיתוף הפעולה.

3. מתודת דירוג ממצאי הביקורת

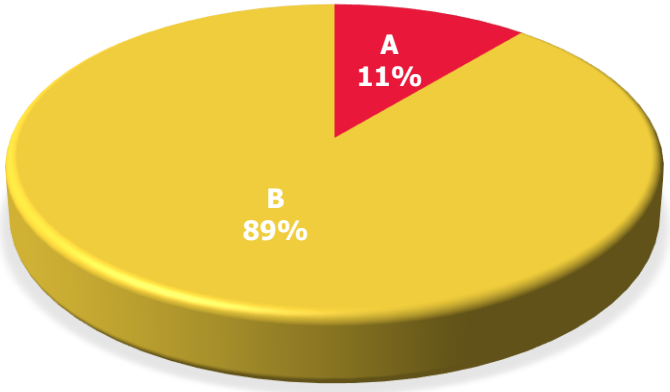
ממצאי הדוח דורגו לאחת מבין שלוש רמות על-פי הערכת הביקורת ובהתאם לפירוט שלהלן:

דירוג	חשיבות	הסבר
A	**גבוהה**	חולשה החושפת לסיכונים מהותיים, להפסד, תרמית, התנהגות בלתי הולמת, בזבוז משאבים ו/או לפגיעה ביכולת השגת יעדי הארגון. בגין חולשה מסוג זה נדרש לתת מענה מיידי לתיקון הליקוי ולטיפול בבקרות.
B	**בינונית**	חולשה לא מהותית בבקרה המביאה לחשיפה של מעגלי פעילות מסוימים בארגון לסיכונים שונים ו/או לפגיעה ביכולת להשיג את יעדי הפעילות. בגין חולשה מסוג זה נדרש לתת מענה מהיר לתיקון הליקוי ולטיפול בבקרות.
C	**נמוכה**	נושא שאינו בעל השפעה מהותית, אולם יכול להשיא ערך מוסף לארגון על ידי שיפור הבקרות הקיימות ו/או על ידי הזדמנות לשפר את היעילות ו/או המועילות.

מפת ממצאי הביקורת

פירוט הפרקים בדוח	A	B	C
1. מיפוי, מדיניות ואסטרטגיה	1	-	-
2. נהלי עבודה	-	1	-
3. צוות מחשוב	-	1	-
4. היבטי חומרה	-	1	-
5. מאגרי מידע והתוכנות בארגון	-	1	-
6. התקשרות עם ספקי התוכנה והשירות	-	1	-
7. הרשאות גישות וסיסמאות	-	1	-
8. אבטחת מידע	-	1	-
9. גיבויים, התאוששות מאסון ותיעוד	-	1	-
סה"כ	**1**	**8**	**0**

התפלגות ההמלצות



סיכום

בעידן הנוכחי של הקדמה הטכנולוגית, מערכות המידע הממוחשבות מהוות חלק בלתי נפרד מפעילויות הארגון. פגיעה בחיסיון המידע, בשלמותו או בשרידותו עלולה לגרום נזק לארגון וגם לגורמים שפרטיהם כלולים במאגרי המידע, ולפיכך חלים על הארגון חוקים ותקנות הנוגעים לאבטחת המידע. בהם חוק הגנת הפרטיות התשמ"א -1981 ("להלן: "החוק") ותקנות הגנת הפרטיות (אבטחת מידע), תשע"ז – 2017 (להלן: "התקנות"), חוק המחשבים התשנ"ה - 1995 ועוד.

הביקורת העלתה כי לא נקבעה מדניות ואסטרטגיה לניהול מערכות המידע בארגון, ולא נערך סקר סיכונים.

הנקודות העיקריות שעלו לשיפור אבטחת המידע כוללות את הצורך בניהול הרשאות, מינוי מנהל מאגר מידע, החלפת סיסמאות, למנוע חיבור התקנים ניידים לרשת, מתן הדרכות לעובדים חדשים והדרכות תקופתיות לכלל העובדים בנושא אבטחת מידע ועוד.

ממצאי הביקורת

1. מיפוי, מדיניות ואסטרטגיה

ממצאים	המלצת הביקורת	
בהתאם לנתונים שהתקבלו מהארגון_בארגון אחזקות משקי דרום ישנם כ-30 משתמשים בעלי הרשאות ברמות שונות. מערכות התקשורת והמחשוב מתופעלות על ידי ספק חיצוני (חברת "ג'יני") החל משנת 2022. במועד הביקורת האחריות על מערכות המידע והקשר עם חברת ""ג'יני" הינו של הכלכלן המוגדר גם כאחראי מערכת המחשוב. לביקורת נמסר כי עם סיום שלב ההקמה/עדכון מערכות המידע בהנהלת חשבונות יבחן מחדש מיקום התחום במבנה הארגוני, לרבות כפיפות ואחריות וכן תבחן האפשרות למנות אחראי תחום תקשורת. <u>מיפוי מערכת המאגר וביצוע סקר סיכונים</u> בהתאם להנחיות פרק 5 בתקנות בארגון קיים מיפוי משתמשים, תוכנות, הרשאות ומדפסות בארגון. הכולל את מבנה מאגר המידע, רשימת מצאי של מערכות המאגר לרבות תשתיות וחומרה, סוגי רכיבי תקשורת, מערכות התוכנה המשמשות להפעלת המאגר, תוכנות וממשקים המשמשים לתקשורת, תרשים הרשת ועוד. בדצמבר 2019 נערך סקר סיכונים על ידי חברת "סופטיקס". ממצאי הסקר העלו כי הארגון ברמת סיכון גבוהה של השתלטות מרחוק, פגיעה בזמינות המערכת ואובדן נתונים, לא קיימות בקרות יעילות בארגון וכי החשיפה הגבוהה ביותר לארגון היא בפגיעה בחומרה שתביא לפגיעה משמעותית ביכולת הארגון לתפקד. בהתאם פעל הארגון לצמצום הסיכונים. חברת "ג'יני" ערכה סקר סיכונים, המראים כי לארגון כלים להתמודד עם האיומים על מערכות המידע. **ממועד זה (2019) לא בוצע סקר סיכונים, נציין כי נהוג לבצע סקר אחת לשנה-שנתיים בהתאם לסיווג הנתונים ולחוסן מערך האבטחה של הארגון.** <u>מדיניות ואסטרטגיה</u> פרק 4 בתקנות הגנת הפרטיות, מחייב כל בעל מאגר מידע לקבוע נוהל אבטחת מידע שיכלול בין היתר, הוראות בעניין אבטחה פיזית וסביבתית, הרשאות גישה, הוראות למורשה גישה, אמצעים להגנה על מערכות המאגר, פירוט הסיכונים להם חשוף המידע שבמאגר, אופן התמודדות עם אירועי אבטחת מידע ועוד. מטרת מסמך מדיניות בתחום מערכות המידע, היא להגדיר עקרונות וכללים אותם מתווה ההנהלה והמהווים את מסגרת העבודה הכללית לנהלי העבודה הנגזרים מהם. על מסמך המדיניות לכלול התייחסות ליעדי ומטרות יחידת המחשב, עקרונות בתחום אבטחת המידע וכדומה. בבדיקתנו נמצא מסמך, אשר נשלח על ידי חברת "ג'יני" הקובע את מדיניות הארגון בנושא אבטחת מידע. לא נמצא בארגון **מסמך המגדיר את מדיניות הארגון ונוהל עבודה שהופץ לעובדי הארגון בנושא מערכות מידי.** על פי סקר הסיכונים שבוצע ב-2017 על ידי חברת "סופטיקס", נמצא כי הטיפול בשימור הידע הארגוני הוא נושא שקיים בו פער, נמסר לביקורת כי **הטיפול בשימור הידע הארגוני טרם הושלם, לא נמצא כי מונה גורם אחראי לטיפול בנושא.**	1. בכדי לקבוע מדניות ואסטרטגיה לניהול מערכות המידע בארגון יש: • לערוך סקר סיכונים. • לקבוע מדיניות ארגונית ואסטרטגיה בנושא מערכות המידע. <u>תגובת המבוקרים</u> – המלצות מקובלות ויבוצעו.	A

אחראי לביצוע	לוח זמנים לביצוע
מנהל מערכות מידע	מדיניות – סוף 2025 סקר סיכונים – 2026

2. נהלי עבודה

ממצאים	המלצת הביקורת
בארגון קיימים נהלי העבודה הבאים: • נוהל תכנית השקעות לחומרה ותכנה – נכתב ביום 28.9.2016 לביקורת הועברה הצעה לעדכון הנוהל שנערך בשנת 2025, אך **טרם אושרה.** • נוהל גיבוי מחשב – עודכן ביום 06.04.2016. • נוהל רכישת שירותים מספק קווי – עודכן ביום 14.11.2016. • נוהל הרשאות – עודכן בינואר 2018. • נוהל אבטחת מידע – עודכן ביום 7.02.2021 המגדיר את אחראי אבטחת המידע בארגון והתנהלות הארגון והעובדים בנושא אבטחת מידע. **נמצא כי הנהלים שהועברו לביקורת לא עודכנו למעלה מ-3 שנים.**	2. יש לבחון את הצורך בעדכון נהלים אחת לשנתיים, לאשר את הנוהל או עדכנו כנדרש. תגובת המבוקרים – המלצה תבוצע. B

אחראי לביצוע	לוח זמנים לביצוע
מנהל מערכות מידע	2026

3. צוות מחשוב

ממצאים	המלצת הביקורת
נמסר כי מנכ"ל הארגון מינה צוות מחשוב, שעליו להתכנס אחת לשנה לדון בנושאי אבטחת מידע, לקבוע מדיניות ומדניות השקעות, **בפועל הנחיה אינה מיושמת**. לביקורת הוצגו שני סיכומי פגישות, אחד כתמונה של סיכום הדברים על גבי לוח מחיק ואחד שהועבר במייל בשנת 2019. בהם התקבלו החלטות בנושא אבטחה פיזית לכניסה למתחם, חדר שרתים, חסימת התקנים, מדניות החלפת סיסמאות, ניתוק דואר אלקטרוני פרטי, החלפת שרת, הדרכת עובדים ועוד. בבדיקת הביקורת נמצא כי **המלצות לשדרוג ושיפור מערכות ניתנות על ידי חברת "ג'יני" לא נבחנו במסגרת צוות מחשוב.** הרכב הצוות המצוין בסיכום הפגישה כלל את אחראי מערכת המחשוב, סמנכ"ל כספים, מנהלת מטה ומש"א, מנהל המפעלים ונציג של חברת "ג'יני" . נמסר כי לצורך בצוע שינוי תוכנה בהנהלת החשבונות צורפה לצוות מנהלת הנהלת החשבונות ולא זומן מנהל המפעלים. **בבדיקתנו לא נמצא מסמך המציין את הרכב הצוות, מועדי התכנסות, אחריות הצוות (לקבוע מדיניות, מדניות השקעות, הדרכות, קבלת דיווח על אירועי חדירה ועוד) וסמכות.**	3. יש לעגן בכתובים את הגדרת תפקיד צוות מחשוב. לרבות הרכב, מועדי התכנסות, אחריות (לקבוע מדיניות, מדניות השקעות, הדרכות, קבלת דיווח על אירועי חדירה ועוד), סמכות ועוד. כמו כן, יש לדון בצוות מחשוב בהמלצות לשדרוג ושיפור מערכות ניתנות על ידי חברת "ג'יני". תגובת המבוקרים – המלצה תבוצע. B

אחראי לביצוע	לוח זמנים לביצוע
מנהל מערכות מידע	עד סוף שנת 2025

4. היבטי חומרה

ממצאים	המלצת הביקורת	
סעיף 6 לתקנות מחייב שמירה פיזית של תשתיות ומערכות החומרה המשמשות את מאגרי המידע, במקום מוגן המונע כניסה אליו ללא הרשאה. מבדיקתנו עולה כי הרשת הארגונית מנוהלת בענן והשרתים נמצאים במשרדי הארגון. השרתים נמצאים בחדר ממוגן אשר הכניסה אליו היא באמצעות מפתח. לביקורת נמסר כי ישנן שתי מפתחות המוחזקים על ידי מזכירת הארגון ועובדת הנהלת החשבונות, **במגירה במשרדן שאינה נעולה.** החדר מתוחזק על ידי חברת "ג'יני" . בבדיקת הביקורת נמצא כי החדר בו נמצאים השרתים משמש **כחדר אחסון**. ישנם 4 שרתים נמצא להם קיים גיבוי (UPS) במקרה של הפסקת חשמל: • שרת של מטריקס – דרכו מנוהלת תוכנת "דנה" • שרת דרכו מנוהלת תוכנת פריוריטי • שרת המשמש כאקטיב דירקטורי • שרת של משקי דן סעיף 6 לתקנות ממשיך ומתייחס למאגרי מידע ברמת אבטחה בינונית ומדגיש את הצורך בנקיטת אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויות המערכות המפורטות לעיל ושל הכנסה והוצאה של ציוד אל מערכות המאגר ומהן. בבדיקתנו נמצא כי באמצעות ניהול הרשת הארגונית בענן עונים על הדרישה לבקרה אחר הכניסה והיציאה מאתרים, עם זאת **לא קיימת מצלמה המתעדת כניסה ויציאה מהחדר**. נציין כי בסקר שבוצע צוין שיש להתקין מצלמה **המתעדת כניסה ויציאה מהחדר**, **מעיון בסכום פגישה של צוות מחשוב עולה שהוחלט שלא ליישם את הנחיה.** ציוד המחשוב בארגון הכולל, בין היתר, תחנות עבודה/ מחשבים אישיים, מדפסות המחוברות לרשת המשותפת, ציוד תקשורת ואבטחת מידע. מרבית הציוד הינו בבעלות הארגון למעט המדפסות. הביקורת קיבלה מיפוי משתמשים וחומרה כנדרש. להלן היבטי חומרה מרכזיים בארגון והאחראי לתפעולם: • מחשבים וציוד בארגון - מסופקים על פי דרישות הארגון ובהתאם לצרכיו, באמצעות חברת "ג'יני" (לה זכות סירוב ראשונה). בבדיקת הביקורת נמצא כי ישנם 19 עובדים להם שויך מחשב נישא מטעם הארגון ומתוכם 3 להם יש מדפסת מטעם הארגון בבית. בנוסף, ל-9 עובדים יש מכשיר טלפון נייד מטעם הארגון. • שרת הדואר אלקטרוני (365) באחריות חברת "ג'יני" .	4. בכדי למקסם את השמירה הפיזית של תשתיות ומערכות החומרה, יש: • לשמור את המפתח לחדר השרתים במקום מאובטח. תגובת המבוקרים – המלצה מקובלת • לוודא כי חדר השרתים ישמש באופן ייעודי ובלעדי את השרתים של הארגון. תגובת המבוקרים – הנושא ייבחן. כרגע אין מיקום אחר לאחסון כספת הנהלת החשבונות ולכן הנושא ייבחן בנפרד • להתקין מצלמה שתתעד כניסה ויציאה מחדר השרתים. תגובת המבוקרים – המלצה תבחן ליישום.	B

אחראי לביצוע	לוח זמנים לביצוע
מנהלת מטה ומש"א	2026

5. מאגרי המידע והתוכנות בארגון

ממצאים	המלצת הביקורת	
להלן מערכות המידע והתוכנות המרכזיות בארגון, לרבות מאגרי המידע המנוהלים בארגון, תוך התייחסות לגורם האחראי: <u>MICROSOFT 365 – מערכת המחשוב הארגונית</u> תיבות הדואר הארגוניות הן דרך תכנת MICROSOFT 365. ישנם 20 משתמשים רשומים, להם משויכת תיבת דוא"ל ארגונית. ההנחיה לפתיחת/סגירת משתמש ניתנת על ידי מנהלת המטה ומש"א לחברת "ג'יני". גיבויים לענן נעשים בסוף כל יום. שרת הקבצים ממוקם בחדר השרתים במשרדי הארגון ומתוחזק על ידי חברת "ג'יני" . <u>פריוריטי – הנהלת חשבונות</u> מערכת ERP המשמשת את הנהלת החשבונות. עומדת עצמאית ומשמשת את הנהלת חשבונות בלבד. במועד הביקורת תהליך הטמעת התוכנה נמצא בתהליך, עד מועד הביקורת הסבו 23 תאגידים לתוכנה. <u>מכפל – תכנת שכר</u> משמשת לרישום שעות עבודה של העובדים והפקת תלושי שכר. <u>עוקץ – תכנת שעוני נוכחות</u> משמשת לדיווחי נוכחות של העובדים. <u>APRICOT – תכנת ניהול כח אדם</u> התוכנה משמשת את מנהלת משאבי אנוש. תוכנה זו איננה מתוחזקת על ידי חברת "ג'יני" ואינה נכללת בהסכם שירותים עם החברה. **דבר העלול להוביל לאבדן נתונים ולזליגת מידע**. חברת "ג'יני" מתפעלת עבור את הארגון את התוכנות (מלבד תוכנת APRICOT), אולם אינה רוכשת אותן עבורה.	5. יש לתפעל ולתחזק את כלל התוכנות ובהם תוכנת ניהול כח האדם APRICOT בעזרת חברת "ג'יני". <u>תגובת המבוקרים</u> – המלצה לתפעל ולתחזק את תוכנת ניהול כח האדם, לא תיושם. מאחר והארגון בוחן מערכת חדשה לטובת הצרכים הקיימים בארגון.	B

אחראי לביצוע	לוח זמנים לביצוע
מנהלת מטה ומשא בתמיכת מנהל מערכות מידע	רבעון ראשון 26

6. התקשרות עם ספקי התוכנה והשירות

ממצאים	המלצת הביקורת	
סעיף 15 (א) בתקנות הגנת הפרטיות עוסק בהתקשרות עם גורמי מיקור חוץ בהיבטי אבטחת המידע וקובע כי מתן גישה לגורם חיצוני יוצר סיכונים מיוחדים, ולכן מצריך בחינת סיכוני אבטחת המידע האפשריים הכרוכים בהתקשרות לרבות לאילו מערכות מידע הוא רשאי לגשת, מה סוג העיבוד שהוא רשאי לבצע ולאלו מטרות ועוד. בהתאם להנחיות, יש לבחון, לפני ביצוע ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות, ואם הם גבוהים מדי בהתחשב ברגישות המידע, להגדיר היטב את טיב ההתקשרות ואף להימנע ממיקור החוץ לחלוטין. הביקורת בחנה את התקשרות הארגון עם ספקים ונותני שרות, להלן ממצאנו: חברת "ג'יני" - אחראית לתפעול מערכת המחשוב ואבטחת המידע בארגון. לביקורת הוצג הסכם חתום בין הארגון לחברת "ג'יני". ההסכם, נחתם בשנת 2022, לשנה, ההסכם מחודש באופן אוטומטי. תכולת השירותים המפורטת בהסכם הינה: • תחזוקה של מערכת המחשוב במשרדי הארגון. • שירות ותמיכה לשרתי ורשתות הארגון לרבות גיבויים, ניהול FIREWALL, VPN, הגנה מפני וירוסים ושליטה ובקרה. • שירות ותמיכה בתוכנות. • סיוע בשחזור קבצי מידע (במידת הצורך). • עדכוני תוכנה. • ניהול שוטף של המשתמשים בארגון. נציין כי בהסכם, מוחרג נושא ניהול מאגרי המידע ועל פיו חברת "ג'יני" אינה אחראית למידע בארגון בשום אופן. רכישת חומרה – נמסר כי לפני רכישת ציוד מחשוב נלקחות שתי הצעות מחיר, אחת מחברת "ג'יני" והשנייה מספק נוסף. אחראי מערכת המחשוב מאשר את הרכישה. מבדיקתנו עולה כי במהלך השנתיים האחרונות כלל ציוד המחשוב נרכש מחברת "ג'יני" גסטטנרטק - חברת אספקה ומתן שירות למדפסות בארגון. נמצא כי קיים הסכם חתום בין החברה לארגון החל מיולי 2023 (לתקופה של 60 חודשים). במסגרת ההסכם, ניתן לארגון שלוש מדפסות בעבור דמי שכירות חודשיים ופעימות מונה (צילומים) להדפסה בשחור לבן והדפסה צבעונית. החברה מתפעלת את המדפסת ובמקרה של תקלה ניתן שירות על ידי טכנאי במשרדי הארגון. על פי ההסכם שוכר הארגון את המדפסות הנ"ל: • מדפסת 1333 CANNON • 2 * מדפסת 5332-TA		
	אחראי לביצוע	לוח זמנים לביצוע

7. הרשאות גישות וסיסמאות

ממצאים	המלצת הביקורת	
סעיפים 7-9 בתקנות מפרטים את החובה הקיימת על בעל מאגר מידע בכל הנוגע לניהול הרשאות גישה למאגרי המידע. בין היתר נקבע בתקנות כי, בעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות תפקיד, הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד. עוד נקבע כי בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם ושל בעלי ההרשאות הממלאים תפקידים אלה וינקוט אמצעים מקובלים בנסיבות העניין ובהתאם לאופי המאגר וטיבו, כדי לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות. **בבדיקת הביקורת לא נמצא כי מונה מנהל למאגר המידע הארגוני כמתחייב בחוק.** רשת קווית ארגונית – יש צורך בהגדרת IP ידנית. לכל כתובת יש שם משתמש וסיסמה. כאמור כל המחשבים מוגנים באמצעות שם משתמש וסיסמה. נמצא כי הרשאות הכניסה והשימוש למערכת הינן אישיות ומורכבות מאותיות ומספרים ומתחלפות מדי שלושה חודשים. הרשאות כניסה לרשת הארגונית בארגון מבוצעת על ידי חברת "ג'יני" בהתאם להנחיות פתיחת משתמשים וסגירת משתמשים הניתנת על ידי מזכירת הארגון או על ידי מנהלת המטה ומשאבי אנוש. **לא נמצא בבדיקתנו תיעוד להנחיות לפתיחת וסגירת משתמשים, נמסר כי הנחיות לחברת "גיני, ניתנות בעל פה או בדואר אלקטרוני.** רשת אלחוטית – ישנן שתי רשתות בארגון, אורחים (GUEST) ורשת ארגונית מאובטחת. לביקורת נמסר כי סיסמאות הכניסה חולקו לכלל העובדים אולם הוחלט לקיים ביקורת הדוקה יותר על הנושא והסיסמה לרשת המאובטחת שונתה וניתנה רק למספר מצומצם של עובדים בארגון. **נמסר כי הסיסמה לרשת האלחוטית אינה מוחלפת מדי תקופה**. תכנת עוקץ – הכניסה לתכנה מתבצעת **ללא צורך בסיסמה.** תכנת מכפל – הכניסה לתכנה מתבצעת באמצעות שם משתמש וסיסמה. בבדיקת הביקורת נמצא כי לכלל המשתמשים בתכנה **יש את אותו שם משתמש והסיסמה**. תכנת פריוריטי – הכניסה לתכנה הינה באמצעות שם משתמש וסיסמה אישיים. הסיסמה מתחלפת מדי 6 חודשים באופן אוטומטי. מנהלת החשבונות בארגון קובעת את הרשאות הגישה של המשתמשים בארגון. למשקים המשויכים בארגון קיימת הרשאת צפייה בדוחות – כרטסות, יתרות, הלוואות ועוד. כל קיבוץ יכול לצפות רק בנתונים המשויכים אליו. לא נמצא כי **העובדים נדרשו לחתום בהסכם על שמירת סודיות המידע.**	6. בכדי למקסם את ניהול ההרשאות, יש: • למנות מנהל מאגר מידע כמתחייב בחוק. • לשמור תיעוד להנחיות לפתיחת וסגירת משתמשים. • להחליף אחת לתקופה שתקבע את הסיסמה לרשת האלחוטית. • לבחון כניסה לתכנת עוקץ בסיסמה. • לתת הרשאות אישיות לתכנת מכפל. • להחתים את העובדים על הסכם שמירת סודיות המידע. תגובת המבוקרים – המלצות יבוצעו.	B

אחראי לביצוע	לוח זמנים לביצוע
מנהל מערכות מידע בעזרת חברת גיני, ומנהלת מטה ומש"א	2026

8. אבטחת מידע

ממצאים	המלצת הביקורת	
סעיף 4 לתקנות מחייב את בעל המאגר לקבוע מסמך ארגוני שמטרתו לפרט נוהל אבטחה ארגוני המייצר מדיניות אבטחה להתמודדות עם סיכוני האבטחה להם חשוף המידע הארגוני. **כאמור, בארגון קיים נוהל אבטחת מידע אולם הוא לא עודכן משנת 2021** (ראה המלצה 2). אבטחת המידע מתחלקת למספר מרכיבים עיקריים: אבטחה לוגית וטכנולוגית, אבטחה פיזית וסביבתית ואבטחת מידע בניהול כח אדם. אבטחה לוגית וטכנולוגית - כאמור לעיל כל כניסה לתחנת עבודה מחייבת שימוש בסיסמה. בנוסף, בשרתים המשרתים את הארגון מותקנת תוכנת firewall מסוג FORTIGATE - מערכת הנוטרת באופן קבוע ומרחוק על ידי חברת "ג'יני" . בנוסף, מופעלת מדיניות גישה לתכנים ואתרים לא מורשים. Firewall (חומת אש) מהווה חיץ ביקורתי בין המחשב לבין החוץ כדוגמת רשת האינטרנט ומטרתה למנוע חדירה של התקשרויות זדוניות, לדוגמה ניסיון התפשטות של וירוס, המגיע מחוץ לרשת המוגנת. על פי בדיקת הביקורת, לא היו ניסיונות חדירה בשנים האחרונות. חיבור מרחוק – מתבצע אך ורק על ידי VPN בהזדהות כפולה (2FA) וניתן לעובדים באישור בכתב מהמנהל הישיר. אבטחה פיזית וסביבתית – של מערכות החומרה המשמשות את מאגרי המידע במקום מוגן המונע כניסה אליו ללא הרשאה. בבדיקה שערכה הביקורת במשרדי הארגון נמצא כי הכניסה לחדר השרתים נעשית באמצעות מפתח. בארגון מותקנת תוכנת אנטי – וירוס ESET הכוללת בתוכה רכיב EDR שמזהה ומגיב אוטומטית לכל ניסיון התקפה על מחשבים אנטי-וירוס זה מנותר ומעודכן ברמת zero trust . בארגון מופעל גם מערכת סינון אימייל ופישיינג מסוג GSPAM החוסמת את האיומים הללו ע"י סריקה וסינון לפני הגעת האימיילים לארגון ומשלוח דוח יומי לכל משתמש ולארגון ליידע על חסימות שבוצעו. כמו כן, בבדיקתנו נמצא כי **ניתן לחבר למחשבים המחוברים לרשת הארגונית התקנים ניידים כדוגמת דיסקאונקי, טלפון נייד, אמצעי מדיה ועוד**. נציין כי באמצעות התקנים אלו ניתן להכניס לרשת וירוסים, "תולעים", אמצעים העלולים להשתלט על המחשב ולשאוב מידע ארגוני שלא לשימוש הארגון. בנוסף, על ידי אמצעים אלו ניתן אף להעתיק מידע לשימוש שאינו מורשה. אבטחת מידע בניהול כח אדם - סעיף 7 לתקנות מדגיש שהגורם האנושי מהווה סיכון משמעותי בתחום אבטחת המידע ומציין את הצורך בקיום הדרכות לבעלי ההרשאות, טרם גישתם למידע ממאגר המידע. **נמסר לביקורת כי לא ניתנה הדרכה לעובדים חדשים.** כמו כן, במאגר ברמת אבטחה בינונית יש לקיים הדרכה תקופתית (שתכלול ריענון על איומי אבטחה חדשים ודרכי התגוננות), לפחות אחת לשנתיים. נמסר כי למרות שקיים נוהל אבטחת מידע **לא התבצעה הדרכת עובדים מעל שנתיים.**	7. בכדי למקסם את אבטחת המידע, יש: • למנוע חיבור התקנים ניידים לרשת כדוגמת דיסקאונקי, טלפון נייד, אמצעי מדיה ועוד. • מתן הדרכות לעובדים חדשים בנושא אבטחת מידע, טרם גישתם למידע ממאגר המידע. • מתן הדרכה תקופתית בנושא אבטחת מידע (שתכלול ריענון על איומי אבטחה חדשים ודרכי התגוננות), לפחות אחת לשנתיים. תגובת המבוקרים – המלצות יושמו.	B

אחראי לביצוע	לוח זמנים לביצוע
מנהל מערכות מידע	2026

9. גיבויים, התאוששות מאסון ותיעוד			
ממצאים	**המלצת הביקורת**		
כל הנתונים או מגובים בענן ו/או מאוכסנים בענן אם זה האימיילים ב365 ואם זה גיבוי של כל המכונות בגיבוי ענן מסוג אקרוניס ניתן לשחזר את הנתונים במלואם מהענן גם אם המערכת קרסה לחלוטין. במקרה של קריסה טוטלית ישנן שתי אפשרויות לשחזור: א. רכישה של שרתים פיזיים חדשים ושחזור מהגיבוי. ב. המרה של הגיבויים בענן לשרתים בענן וחיבור ישירות אליהם. במקרה של מחיקה של קבצים בודדים ע"י משתמש ניתן לשחזר ישירות ממערכת SC במיידי. תיעוד של אירועי אבטחה מנוטר מדי יום ומופק דוח יומי המסכם את אירועי היום על פי: שם המשתמש, תאריך גיבוי, תוצאת הגיבוי, סטטוס אבטחת מכשיר, מועד הגיבוי הבא, מספר הגיבויים, מספר ההתראות שהתקבלו וסיבתן. השרתים מגובים על ידי ספק כח עצמאי (UPS), אולם ספק זה יכול לתת גיבוי לזמן קצר וקצוב (30 דקות), **לא נמצא כי קיים גיבוי להפסקות חשמל ארוכות זמן.**	8. מומלץ לוודא כי קיים גיבוי לטווח ארך למערכות השונות ולשרתי הארגון במקרה של הפסקות חשמל ארוכות זמן. <u>תגובת המבוקרים</u> – המלצה מקובלת		B
	אחראי לביצוע	לוח זמנים לביצוע	
	מנהל מערכות מידע בעזרת ג'יני ומנהל תשתיות ואחזקה	2026	

* * *

תודה רבה