



מבקר המועצה

דוח על הביקורת

במועצה המקומית יבנאל

לשנת 2020

דוח מס' 20

מ.מ. יבנאל, ניסן תשפ"א – מרץ 2021

תוכן עניינים:

3	הקדמה
	<u>דוחות הביקורת:</u>
4-18	יישום תקנות אבטחת המידע - מ.מ. יבנאל
19-22	<u>קרנות פנסיה וגמל</u> - יישום הוראות החוק וההסכמים הקיבוציים ע"י הרשות המקומית
23-27	תקן כ"א המועסק בבתי הספר ביבנאל, לעומת תקצוב משרד החינוך

28-30	מעקב אחר תיקון ליקויים קודמים

הקדמה :

בדוח זה נכללים ממצאי ביקורת שונים על פעילות הרשות המקומית. הנושאים המרכזיים שנבדקו :

• יישום תקנות אבטחת המידע – מ.מ. יבנאל:

בחודש מאי 2018 נכנסו לתוקף תקנות הגנת הפרטיות (אבטחת מידע). התקנות חלות על כל המשק הישראלי, והן מבקשות להגן על האנשים שמידע אודותיהם קיים במאגר המידע. התקנות קובעות שלוש רמות של מאגרי מידע, עליהן חלות רמות אבטחה שונות, בהתאם לסיכוני האבטחה שהם מייצרים. בכפוף לתקנות אבטחת המידע, נמצא כי על המועצה המקומית יבנאל - חלה רמת האבטחה הבינונית (רמת האבטחה החלה על הרשויות המקומיות). המבקר בדק את היערכות הרשות המקומית ליישום ההוראות ועמידה בתקנות אבטחת המידע הנדרשות.

• קרנות פנסיה וגמל- יישום הוראות החוק וההסכמים הקיבוציים ע"י הרשות המקומית:

במסגרת ההסכמים הקיבוציים החלים על עובדי הרשויות המקומיות- זכאים העובדים להפרשות לקרנות פנסיה וקופות גמל. נבדק האם הרשות המקומית מיישמת את ההוראות והכללים בנושא בכל הקשור לחובת הרשות המקומית לתפוח קרנות פנסיה וקופות גמל לעובדים המועסקים על ידה.

• תקן כ"א המועסק בבתי הספר ביבנאל, לעומת תקצוב משרד החינוך:
לבקשת ראש המועצה, בדק מבקר המועצה את תקן כח האדם המועסק בבתי הספר – "נפתלי" ו-"חב"ד" ביבנאל, לעומת תקן/תקצוב משרד החינוך את המוסדות הללו.

• מעקב אחר תיקון ליקויים קודמים.

בברכה
שמעון דיין
מבקר המועצה

**יישום תקנות אבטחת
המידע
מ.מ. יבנאל**

דוח ביקורת:

אבטחת מידע – מועצה מקומית יבנאל

כללי:

אבטחת מידע פירושה הגנה על שלמות המידע והגנה עליו מפני חשיפה, שימוש או העתקה, על ידי גורמים שאינם מורשים.

בחודש מאי 2018 נכנסו לתוקף- תקנות הגנת הפרטיות (אבטחת מידע). התקנות חלות על כל המשק הישראלי, והן מבקשות להגן על האנשים שמידע אודותיהם קיים במאגר המידע. התקנות קובעות שלוש רמות של מאגרי מידע, עליהן חלות רמות אבטחה שונות, בהתאם לסיכוני האבטחה שהם מייצרים.

בתקנות נקבע כי על מאגרי מידע שיובאו להלן, חלה רמת האבטחה הבינונית:

- מאגר מידע שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק, לרבות שירותי דיוור ישיר.
- מאגר מידע שבעליו הוא גוף ציבורי (משרדי הממשלה, רשות מקומית וכו').
- מאגר מידע הכולל מידע על צנעת חייו האישיים של אדם, מידע רפואי, מידע גנטי, מידע על דעות פוליטיות, מידע על עבר פלילי, נתוני תקשורת, מידע ביומטרי, מידע על נכסיו של אדם, הרגלי צריכה וכו'.

בכפוף לתקנות אבטחת המידע, נמצא כי על המועצה המקומית יבנאל - חלה רמת האבטחה הבינונית {רמת האבטחה החלה על הרשויות המקומיות}.

מטרת הבדיקה, לבדוק את היערכות הרשות המקומית ליישום ההוראות ועמידה בתקנות אבטחת המידע הנדרשות.

ממצאים:

1. מינוי ממונה על אבטחת מידע, ומנהל מאגרי מידע ברשות המקומית:

חוק הגנת הפרטיות קובע כי, גוף ציבורי {להלן: רשות מקומית} נדרש למנות ממונה על אבטחת מידע:

- הממונה יהיה כפוף ישירות למנהל מאגר המידע או המחזיק, למנהל בכיר אחר הכפוף לו, או למנכ"ל הארגון {תקנה 3(1)}.
- הממונה יכין תוכנית לבקרה שוטפת על העמידה בדרישות התקנות, יבצע אותה ויודיע להנהלת הארגון ולמנהל המאגר על ממצאיו {תקנה 3(3)}.
- הממונה על האבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו {תקנה 3(4)}.

ממצאים:

1.1. הרשות המקומית לא מינתה מנהל למאגרי המידע במועצה. משכך, מנכ"ל המועצה הוא למעשה מנהל מאגרי המידע, הלכה למעשה.

1.2. הרשות המקומית לא מינתה ממונה על אבטחת המידע במועצה.

על הרשות המקומית לפעול למינוי ממונה אבטחת המידע במועצה, שיהיה כפוף למנהל מאגרי המידע במועצה. נדרש למנות אדם מקצועי לתפקיד – יש לשקול מינוי במיקור חוץ.

1.3. בנוהל האבטחה של מאגרי המידע- נקבעו סדרי בקרה כנגד פגיעה בשלמות המידע- אותן נדרש הממונה על אבטחת המידע לבצע ולבדוק בהתאם לנוהל.

לא קיימת תוכנית עבודה שנתית – בה מפורטים הפעולות אותן נדרש לבצע על בסיס קבוע במהלך העבודה השוטפת.

2. מיפוי, סיווג ורישום מאגרי המידע ברשות המקומית:

במסגרת תקנות אבטחת המידע, נדרשת הרשות המקומית לבצע מיפוי של מאגרי המידע המצויים ברשותה - סיווג המאגרים, מינוי מנהל למאגר, רישום המאגר כנדרש בחוק, והפקת מסמך אב המאגד בתוכו את הגדרות המאגר, בכפוף להוראות, כל מאגר בנפרד.

ממצאים:

2.1. נמצא כי **הרשות המקומית לא ביצעה מיפוי של מאגרי המידע שברשותה.**

2.2. **אין בידי הרשות המקומית רשימה מעודכנת של נכסי המידע** {שרתים, מערכות, מיקומן, הגנות וכו'}.

2.3. **לא נקבעו מנהלי מאגר ייעודיים** – עובד רשות מקומית שמאגר המידע קשור לתחום עיסוקו ותפקידו ברשות המקומית.

2.4. **לא הוסדר רישום מאגרי המידע מול רשם מאגרי המידע.**
נדרש לפעול מול היועמ"ש לקידום נושא רישום המאגרים כנדרש בחוק.

2.5. **לא הופק מסמך אב- מסמך הגדרות המאגר, לכל מאגר בנפרד – המכיל את כל ההתייחסויות הנדרשות בתקנות.**

3. נוהל אבטחת מידע ארגוני:

תקנה 4(א-ד), מחייבת את בעל מאגר המידע לקבוע במסמך נוהל אבטחה ארגוני, שמטרתו לייצר מדיניות אבטחה ארגונית להתמודדות עם סיכוני האבטחה להם חשוף המידע.

הנוהל צריך לכלול לפחות את הנושאים הבאים:

- הוראות בעניין אבטחה פיזית.
- הרשאות גישה למאגרי מידע.
- תיאור אמצעי הגנה ובקרה.
- הוראות למורשי גישה.
- סיכונים אליהם חשוף המידע שבמאגרי מידע, במסגרת הפעילות השוטפת.
- אופן התמודדות עם אירועי אבטחת מידע.
- הוראות לניהול התקנים ניידים.
- אמצעי הזיהוי והאימות לגישה למאגרי מידע.
- אופן הבקרה על השימוש במאגרי מידע.
- עריכת ביקורות תקופתיות.
- גיבוי נתונים.

- **נמצא כי הרשות המקומית לא הפיקה נוהל אבטחת מערכות מידע במועצה המקומית יבנאל.**
יש להפיק נוהל כוללני, אשר יתייחס לנושאים הנדרשים בתקנות. כמו כן נדרש להפיץ את הנוהל בקרב מנהלי המחלקות במועצה.

4. אבטחה פיזית וסביבתית – תשתיות ומערכות החומרה של מאגרי המידע:

תקנה 6(א) מחייבת שמירה פיזית של תשתיות ומערכות החומרה המשמשות את המאגר, במקום מוגן המונע כניסה אליו ללא הרשאה. זאת לאור העובדה כי הגדרות הליבה של המערכת ואמצעי ההגנה הלוגיים שלה כפופים לסיכון של שינוי ועדכון באמצעות גישה פיזית, כך גם לגניבת אמצעי אחסון פיזיים.

תקנה 6(ב) קובעת כי נדרש לתעד את הכניסות והיציאות של העובדים מאתרים בהם מצויות המערכות, וכן לתעד הכנסת ציוד אל מערכות המאגר והוצאת ציוד מהן. למשל באמצעות התקנת מצלמות, מערכת זיהוי ביומטרי וכו'.

- 4.1 **לא קיים חדר שרתים- ייעודי.** ארון הבקרה והתקשורת ממוקם במשרד מנהלת לשכת ראש המועצה. לא קיימת בקרת כניסה לחדר זה.
 - 4.2 אין תיעוד כניסה לחדר בו ממוקם השרת – לא הותקנה מצלמה המתעדת את המתרחש בחדר זה.
 - 4.3 **לא קיימים אמצעי אבטחה פיזית בגבולות הרשות:** אין שער כניסה. כניסה לא מבוקרת למועצה, יש שומר בכניסה- אולם אין תשאול בכניסה, ולא רישום הנכנסים.
 - 4.4 קיימות מצלמות ברשות המקומית- בפיקוח מח' ביטחון.
- **המצלמות אינן מנוהלות בהתאם לדרישות חוק הגנת הפרטיות:** רישום כמאגר, יידוע הציבור, נהלים ומורשי חתימה וכו'.

5. אבטחת מידע – ניהול כח אדם:

לנוכח העובדה שהגורם האנושי מהווה גורם סיכון משמעותי בתחום אבטחת המידע, יש לוודא כי ייקלטו לעבודה הקשורה למאגר המידע עובדים המתאימים לעבודה זו, לאחר שנקטו אמצעים סבירים המקובלים בהליכי מיון עובדים ושיבוצם. יש לקחת בחשבון את רגישות המידע שבמאגר ואת היקף הרשאות הגישה לתפקיד שמיועד לו המועמד לתפקיד.

נדרש לבחון גם את מידת התאמתם של העובדים הקיימים בארגון לגישה למאגר המידע.

- יש לקיים הדרכות לבעלי הרשאות בנושא החובות לפי חוק הגנת הפרטיות והתקנות, בטרם יקבלו גישה למידע ממאגר המידע או לפני שינוי היקף הרשאותיהם.
- יש לקיים פעילות הדרכה תקופתית אחת לשנתיים לפחות לבעלי הרשאות.

ממצאים:

5.1. כל מועמד לתפקיד ברשות המקומית- עובר תהליך מיון, המבוצע על ידי המנהל הישיר בשיתוף ממונה על המשאב האנושי – מנכ"ל, לרבות: סקירת קורות חיים, בדיקת תעודת המעידות על השכלה או כישורים דרושים, שיחת ממליצים, ועמידה בפני ועדת בחינה- ראיון והתרשמות.
בשקלול כל האמור לעיל, נבחר המועמד לתפקיד המוצע במועצה.
- **לא מתקיימים מבדקי אמינות למועמדים להעסקה** {עובדים חדשים, מיקור חוץ, קבלנים וכ'}.
מיקור חוץ,

5.2. **עובדים חדשים, עובדי קבלן, ומיקור חוץ – לא נדרשים לחתום על הסכמי סודיות ואבטחת מידע כחלק מתנאי ההעסקה שלהם** {למעט עובדים בחוזה אישי}.

5.3. **כיום, לא מבצעת הרשות המקומית הדרכה לעובדים חדשים, בתחום אבטחת המידע, בטרם קבלת הרשאת גישה למאגרי המידע.**

נדרש לקיים הדרכות לעובדים חדשים בנושא החובות החלות על העובד בכפוף לתקנות הגנת הפרטיות, ובכפוף לנוהל אבטחת המידע שנקבע ברשות המקומית.
יש לעגן זאת בנוהל קבלת עובדים לעבודה ברשות המקומית.

5.4. נכון למועד הבדיקה – **טרם התקיימה הדרכה תקופתית לעובדים - בעלי הרשאות גישה למאגרי המידע.**

בכפוף לתקנות- נדרש לקיים הדרכה תקופתית לעובדים בעלי הרשאות גישה למערכות מידע, אחת לשנתיים, לכל הפחות. על הרשות המקומית להיערך לקיום הדרכה לכלל בעלי הרשאות, בהקדם.

מצ"ב:

נספח 1 – נוהל אחריות אישית לאבטחת מידע - להפצה לכלל עובדי המועצה, להם יש נגישות למאגרי מידע. הנוהל מופץ ע"י אגף הסייבר במשרד הפנים ויש להתאימו לאופי המועצה וסדרי עבודתה.
יש להחתים את כלל העובדים על הנוסח המוצע שיותאם לאופי המועצה וסדרי העבודה בה.

6. ניהול הרשאות גישה:

נקבע כי יש לקבוע הרשאות גישה למאגר לכל עובד, רק במידה הנדרשת לו לצורך ביצוע תפקידו. כמו כן נדרש לנהל רשימת הרשאות מעודכנת.

ממצאים:

- לא קיים נוהל הקצאת הרשאות גישה למאגרי המידע לעובדי המועצה. כמו כן לא קיים נוהל לביטול בקרת גישה למשתמשים במערכות ומאגרי המידע.
- לא מתבצעות בקרות הרשאה תקופתית לגישה למאגרי המידע.
- לא מתקיימות בקרות תקופתיות לביטול הרשאות ובחירת סיסמא.

יש להקפיד כי נוהל אבטחת המידע יתייחס בין היתר לנושא הרשאות הגישה, לרבות: חוזק הסיסמה, מספר ניסיונות שגויים, תדירות החלפת הסיסמאות, ניתוק ואופן טיפול בתקלות הקשורות באימת זהות המשתמש.

7. זיהוי ואימות גישה למאגרי המידע:

תקנה 9(א) | קובעת כי יש לוודא שמי שניגש למידע במאגר הוא עובד מורשה, ולכן יש לאמת את זהותו באמצעים מקובלים בנסיבות העניין. לפחות באמצעות סיסמה.

תקנה 9(ב) | אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה. בנוהל האבטחה יש לקבוע גם את:

- אופן הזיהוי. אם אופן הזיהוי מבוסס על סיסמאות – הנוהל יתייחס לחוזק הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד מורשה הגישה, ובכל מקרה לתקופה שלא תעלה על 6 חודשים.
- ניתוק אוטומטי לאחר פרק זמן של אי-פעילות.

תקנה 9(ג) | בעל המאגר ידאג לביטול ההרשאות של בעל ההרשאה שסיים את תפקידו, ובמידת האפשר לשינוי סיסמאות, מיד עם סיום תפקידו של בעל ההרשאה.

ממצאים:

7.1. נמצא כי גישה למאגר מידע לכל מורשה { בעל תפקיד במועצה } - מחייבת זיהוי ואימות ע"י סיסמה.

7.2. **לא קיים נוהל אבטחת מידע במועצה, הקובע תדירות החלפת סיסמאות ונהלים בנוגע לחוזק הסיסמה,** לרבות בקרה על החלפת הסיסמה וחוזק הסיסמה.

7.3. קיים ניתוק אוטומטי ממאגרי המידע- במערכות החברה לאוטומציה. לא קיים מידע לגבי מאגרי מידע נוספים.

במסגרת הפקת נוהל אבטחת המידע במועצה- הנדרש על פי התקנות – נדרש לקבוע בנוהל, תדירות החלפת הסיסמאות, נהלים בנוגע לחוזק הסיסמה ובקרות.

7.4. **לא קיים נוהל ו/או העברת מידע בנוגע לביטול הרשאת גישה לבעל תפקיד שסיים את עבודתו במועצה.**

נדרש להפיק נוהל { משאבי אנוש } בכל הנוגע להקצאה, עדכון וביטול הרשאות, למאגרי המידע.

8. בקרה ותיעוד גישה למאגרי מידע:

תקנה 10 (א) קובעת כי יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר מנגנון בקרה, אשר יכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

תקנה 10 (ב) קובעת כי על מנגנון הבקרה להיות עצמאי, לפעול באופן רציף, וככל הניתן ללא אפשרות להתערבות חיצונית שתביא לביטול או שינוי בהפעלתו. אם בוצעו שינויים או ביטולים בהפעלת המנגנון, על המנגנון לאתר אותם באופן אוטומטי ולהפיץ התראות לאחראים. תקנה 10 (ג), בעל מאגר המידע נדרש לקבוע נוהל בדיקה שגרתית של נתוני התיעוד של מנגנון הבקרה, ויערוך דו"ח של הבעיות שהתגלו וצעדים שנקטו בעקבותיהן. על מנת לעמוד בחובתו של בעל המאגר לאתר אירועי אבטחה בזמן אמת מומלץ ליישם מנגנונים אוטומטיים להתראה.

ממצאים:

- לא נתקבלו נתונים האם המערכות שבשימוש המועצה, מבצעות רישומי גישות.

נדרש לוודא כי התיעוד האוטומטי לגישה למאגרים - כולל את הדרישות בתקנה 10א'.

יש לקבוע נוהל בדיקה שגרתית של נתוני תיעוד של מנגנון הבקרה. יש להקפיד כי הנתונים ממנגנון הבקרה יישמרו לכל הפחות 24 חודשים.

9. תיעוד אירועי אבטחה:

תקנה 11 קובעת כי במידה ואירע אירוע אבטחה? יש לתעד.
יש להתבסס על רישומים אוטומטיים אודות אירועי אבטחה במערכות המאגר של הארגון.
נדרש לקבוע הוראות לעניין התמודדות עם אירועי אבטחת מידע ואופן הדיווח לבעל המאגר.
בעל המאגר יקיים דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכונו של נוהל האבטחה.

ממצאים:

- נמצא כי בחלק ממערכות המידע – קיים תיעוד אוטומטי.
- לא קיים נוהל אבטחה המתייחס להתמודדות עם אירוע אבטחה.
- לרשות המקומית אין מדיניות וכלים לביצוע סקרי סיכונים בתוך רשות הרשות.
- לא קיימת תוכנית לביצוע ובדיקת מבדקי חדירה ובקורות. כמו כן לא מבוצעים מבדקי חדירה על בסיס תקופתי.

יש לוודא כי בכלל מערכות המידע שבשימוש הרשות המקומית- יהיה תיעוד אוטומטי לאירועי אבטחה.
נדרש לקבוע הגבלות גישה לנכסי המידע, וקביעת מדיניות לביצוע ביקורת על הגבלות הגישה { לרבות מבדקי חדירה יזומים }.
יש לקיים דיון אחת לשנה לכל הפחות, בנושא אירועי אבטחה, ולהפיץ מידע בנדון לעובדי הרשות המקומית.

10. שימוש בהתקנים ניידים:

התקן נייד הוא מחשב או התקן אחסון המיועד לשימוש נייד. קיים סיכון כי מידע מהמאגר עלול לדלוף החוצה באופן לא מורשה, או שחיבור ההתקן הנייד יגרום נזק למערכות המאגר בשל נזקה המותקנת בו. חשוב להגביל את האפשרות לחבר התקנים ניידים למערכות המאגר, בשים לב לרגישות המידע שבו. אם אפשר לחבר התקנים ניידים למערכת, חשוב להגן על המידע המועתק אליהם. הצפנת המידע, על ידי שימוש בשיטות הצפנה מקובלות, תיחשב נקיטת אמצעים סבירים.

ממצאים:

- לא קיימת מגבלה לחיבור התקנים ניידים.
- לא קיימים נהלים בנושא.

נדרש ליידע את עובדי הרשות המקומית בדבר הסיכונים הכרוכים בשימוש בהתקנים ניידים.
יש להנחות את כלל העובדים שלא לשמור בהתקנים ניידים- מידע ממאגרי מידע או חלקים מהם, ולהמעיט שימוש בהתקנים ניידים.
נדרש להוציא הנחיות בנדון.

11. ניהול מאובטח ומעודכן של מערכות המאגר:

תקנה 13 (ג) קובעת כי בעל המאגר נדרש לעדכן באופן שוטף את מערכות המאגר, חומרה ותוכנה בהתאם להנחיות היצרן על מנת לנטרל פגיעויות וחולשות המתגלות מעת לעת.

ממצאים:

- הציוד אינו מתוחזק בהתאם להנחיות היצרן ואין הסכמי שרות תחזוקה {עדכונים, אחריות, ביטוח}.
- הרשות המקומית אינה מקפידה להפסיק שימוש במערכות שהיצרן הפסיק את התמיכה בהיבטי האבטחה שלהן.

נדרש בדיקת תוקף הסכמים לשירותי תחזוקה של הציוד ברשות המקומית.
קיומם של הסכמים לתחזוקת ציוד בהתאם להנחיות היצרן.

12. אבטחת תקשורת:

אם מערכות המאגר מחוברות לרשת האינטרנט או לרשת ציבורית אחרת, נוצר סיכון של גישה חיצונית ולא מורשית אליהן.

תקנה 14 קובעת כללים בנדון:

התקנת אמצעי הגנה מפני חדירה לא מורשית, או תוכנות מזיקות .
העברת מידע ממאגר המידע, ברשת הציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.

במאגר מידע שניתן לגשת אליו מרחוק ("חיבור מהבית" למשל), ייעשה שימוש באמצעים שמזהים את המתקשר והמאמתים את זהותו.

ממצאים:

- נדרש לוודא כי קיימים אמצעי הגנה מפני חדירה לא מורשית ו/או תוכנות מזיקות.
- במאגרי מידע שניתן לגשת אליהם מרחוק – נעשה שימוש באמצעים המזהים את המתקשר ומאמתים את זהותו.
- **לא קיימת מדיניות אבטחה לאמצעי מחשוב נייד** {מחשבים ניידים, טלפונים ניידים}

נדרש לוודא כי מידע המונגש בממשקים בגישה מרחוק – נעשה בשיטות הצפנה מקובלות.

יש לקבוע מנגנון הזדהות חזק בחיבור לרשת הארגונית מבחוץ.

- **נדרש כתיבת מסמך מדיניות אבטחה לשימוש באמצעי מחשוב נייד {לרבות סיסמה מורכבת, אנטי וירוס והצפנה}.**

מצ"ב:

נספח 2 - הצהרת מחזיק מחשב נייד על אבטחת מידע (נוסח מוצע ע"י אגף הסייבר במשרד הפנים).

יש להחתיים את כלל העובדים {המחזיקים מחשב נייד מטעם המועצה} על הנוסח המוצע שיותאם לאופי המועצה וסדרי העבודה בה.

13. שימוש בשירותי מיקור חוץ לעיבוד מידע אישי:

מתן גישה לגורם חיצוני יוצרת סיכונים מיוחדים, ולכן מצריכה בחינת סיכוני אבטחת המידע האפשריים הכרוכים בהתקשרות עימו.
תקנה 15 קובעת את ההוראות הבאות:

- לבחון, לפני ביצוע ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות, ואם הם גבוהים מדי בהתחשב ברגישות המידע, להימנע ממיקור החוץ לחלוטין.
- לקבוע במפורש בהסכם את כל אלה, בשים לב לסיכוני אבטחת המידע

ממצאים:

- לא קיימת מדיניות ברשות המקומית לניהול מיקור חוץ בכל הנוגע לאבטחת מידע.
- הסכמי התקשרות עם גורמי חוץ הקשורים בגישה, עיבוד, העברה ו/או ניהול של נכסי המידע במועצה – אינם כוללים דרישות אבטחת מידע והגנת הפרטיות.
- לא מוגדרות דרישות אבטחת מידע בעת שדרוג מערכות ובעת רכש של מערכות מידע.
- אין בקרה אחר יישום דרישות אבטחת מידע ורמת האבטחה הנדרשת בהסכמי התקשרות עם ספקים חיצוניים.

נדרש לקבוע בנוהל אבטחת המידע הנחיות בנוגע לסוגיית מיקור חוץ.
נדרש לנסח ו/או לעדכן הסכמים קיימים – בכל הנוגע להיבטי אבטחת המידע, לרבות: הרשאות גישה, סוג העיבוד, משך ההתקשרות, סיום ההתקשרות ואופן יישום הוראות אבטחת המידע.
נדרש להקפיד על כתב התחייבות לשמירת סודיות- חלק בלתי נפרד מהסכם ההתקשרות.
בחינת סיכונים הנובעים מאופי ההתקשרות, והבקורות הנדרשות.

מצ"ב:

נספח 3 - דרישות אבטחת מידע לחוזים עם ספקים חיצוניים (נוסח מוצע ע"י אגף הסייבר במשרד הפנים).

נספח 4 - דרישות אבטחת מספק מחזיק מאגר מידע (נוסח מוצע ע"י אגף הסייבר במשרד הפנים).

נדרש להתאים לאופי המועצה וסדרי עבודתה – להחתים את כלל הספקים הרלוונטיים.

14. ביקורת תקופתית:

תקנה 16 קובעת, כי אחת ל-24 חודשים לפחות יש לערוך ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, שאינו ממונה האבטחה של המאגר, על מנת לוודא עמידתו בהוראות התקנות.

בדו"ח הביקורת ידווח המבקר על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב.

ממצאים:

- נמצא כי **לא בוצעה ביקורת בנושא אבטחת המידע במועצה ע"י גורם חיצוני, הבקי בתחום סיכוני אבטחת המידע.**
- לא מבוצעים מבדקי חדירה על בסיס תקופתי.

הרשות המקומית נדרשת לערוך ביקורת תקופתית בנוגע לאבטחת המידע ברשות המקומית, ע"י גורם בעל הכשרה מתאימה לביצוע הביקורת. כמו כן נדרש לפעול לתיקון כלל הפערים שיתגלו בביקורת, בכפוף להוראות תקנות אבטחת המידע.

15. הקמת ועדה להעברת מידע בין גופים ציבוריים:

העברת המידע בין גופים ציבוריים הוסדרה בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו - 1986. תקנות אלה כוללות את הדרישות במקרים בהם גוף ציבורי מעוניין או נדרש להעביר מידע אל גוף ציבורי אחר. בכל גוף ציבורי אשר מוסר או מקבל מידע יש למנות וועדה להעברת מידע (סעיף 3א לתקנות). תפקידי הוועדה:

- לבחון בקשות למסירת המידע מאת הגוף הציבורי.
- לבחון בקשות לקבלת מידע של הגוף הציבורי מאת גוף ציבורי אחר.
- לקבוע הוראות בעניין הגישה למאגרי מידע שברשות הגוף הציבורי, אשר יבטיחו את השמירה על המידע המצוי בהם.

הרכב הוועדה:

נקבע כי מספר חברי הוועדה לא יפחת משלושה.
יו"ר הוועדה - המנכ"ל או סגנו או עובד בכיר הכפוף לו ישירות. חברי הוועדה יכללו יועץ משפטי או נציגו, ועובדים שתחום עיסוקם בניהול מידע ואבטחתו.

ממצאים:

- **נמצא כי לא מונתה ועדה להעברת מידע, כנדרש בתקנות.**
- **לא נקבעו קריטריונים בעניין כללי הגישה לכל מאגר המצוי ברשות המקומית.**

מצ"ב:

נספח 5 – הוראות משרד המשפטים, בכל הנוגע להקמת ועדה להעברת מידע בין גופים ציבוריים.

**הפרשות הרשות המקומית לקרן פנסיה
וקופות גמל
ש"נ / כוננות / קריאות פתע**

דוח ביקורת:

בדיקת הפרשות הרשות המקומית לקרנות השונות, בכפוף לזכויות

עובדי המועצה:

קרן פנסיה / קופ"ג החזר הוצאות / קרן פנסיה רכיבי עבודה נוספת / קרן

השתלמות:

מבוא:

במסגרת ההסכמים הקיבוציים החלים על עובדי הרשויות המקומיות- זכאים העובדים להפרשות לקרנות פנסיה וקופות גמל.

המבקר בדק האם הרשות המקומית מיישמת את ההוראות והכללים בנושא בכל הקשור לחובת הרשות המקומית לתפוח קרנות פנסיה וקופות גמל לעובדים המועסקים על ידה.

הנושאים שנבדקו:

קרן פנסיה

קופ"ג החזר הוצאות

קרן פנסיה -רכיבי עבודה נוספת

קרן השתלמות

מועד ביצוע הבדיקה: אוקטובר 2020

ממצאים:

1. קרן פנסיה:

הסכם המעבר לפנסיה צוברת קובע כי עובדים שיתקבלו לעבודה ברשות המקומית מהמועד הקובע {01/11/2001} ואילך – עובדים אלו יבוטחו בפנסיה צוברת, בגין כל רכיבי השכר {משכורת קובעת לפנסיה ורכיבים שאינם פנסיוניים, ואשר אינם בגדר החזר הוצאות, גילום מס וזקיפת הטבה למס, ולמעט בגין ביגוד}.

ממצאים:

- נמצא כי הרשות המקומית מקפידה להפריש לכל עובד שמתקבל למועצה לפנסיה צוברת כנדרש.
- במועד ביצוע הביקורת, לכלל העובדים במועצה הופרש לקרן פנסיה כנדרש על פי הנהלים.

2. קופת גמל החזר הוצאות :

הסכם המעבר לפנסיה צוברת קבע חובת תשלום 5%+5% עבור קופת הגמל על רכיבי השכר המוגדרים כ"החזר הוצאות".

עובדים זכאים להפריש לקופת גמל בגין רכיבים שהינם החזר הוצאות { החזר הוצאות רכב קבועות או משתנות, ביטוח חובה לרכב, ביטוח מקיף לרכב, אגרת רישוי לרכב, החזר הוצאות נסיעה, אש"ל, כלכלה, טלפון וכד'}. ההפרשה היא בשיעור של 5% עובד – 5% מעביד.

ממצאים :

למרבית העובדים ברשות המקומית רכיבי שכר המוגדרים "החזר הוצאות". בעיקר החזר הוצאות נסיעה {תחבורה ציבורית} והשתתפות בטלפון. לחלק מן העובדים ישנה השתתפות באחזקת רכב.

- הרשות המקומית מפרישה לעובדיה לקופ"ג החזר הוצ', בגין רכיבי שכר המוגדרים כ"החזר הוצאות".
- נכון למועד הביקורת **נמצא כי ל- 19 עובדים, המועצה אינה מפרישה לקופת גמל – החזר הוצאות { 5% עובד , ו- 5% מעביד } בניגוד להסכם.**

הרשות המקומית נדרשת לערוך מיפוי לכלל העובדים שלא הופרש להם לקופ"ג החזר הוצאות. נדרש להקפיד כי יופרש לכלל עובדי הרשות המקומית, בגין רכיבי שכר, הנכללים בהגדרת "החזר הוצאות", לקופ"ג בכפוף להסכם.

3. קרון פנסיה – רכיבי עבודה נוספת :

בהסכם המעבר לפנסיה צוברת נקבע כי - החל מ- 01/11/2001 יכללו השעות הנוספות {ללא גמל}, בהסדר פנסיה צוברת לכלל עובדי הרשות המקומית {פנסיה תקציבית וצוברת} .

על רכיבי השכר המוגדרים כ"עבודה נוספת" תחול חובת הפרשה לקופת "פנסיה צוברת" הן לעובדים חדשים והן לעובדים ותיקים .

לפיכך, הרשות המקומית נדרשת לבצע - הפרשות וניכויים לפנסיה צוברת בגין כלל רכיבי המשכורת אשר אינם נכללים במשכורת הקובעת לפנסיה, ואשר אינם בגדר החזר הוצאות, גילום מס וזקיפת הטבה למס {שעות נוספות/ שעות כוונות/ קריאות פתע}.

ממצאים:

- נמצא כי הרשות המקומית מפרישה לעובדים המקבלים שעות נוספות ו/או כוננות באופן קבוע, לקרן פנסיה צוברת-רכיבי עבודה נוספת כנדרש.
- במועד ביצוע הביקורת, **נמצאו 6 עובדים המקבלים ש"נ ו/או כוננות ו/או קריאות פתע, באופן קבוע מידי חודש – ולא הופרש עבורם לקרן פנסיה רכיבי עבודה נוספת.**

הרשות המקומית נדרשת לבצע מיפוי של כלל העובדים במועצה, בכל הנוגע לביצוע מרכיבי עבודה נוספת. עובדים המבצעים באופן קבוע- ש"נ/כוננות/קריאות פתע, באופן תדיר - יש להפריש עבורם לקרן פנסיה לרכיבי "עבודה נוספת".

4. קרן השתלמות:

- עובדי הרשויות המקומיות שבדירוג המינהל והשירותים (אחיד) או הדירוגים המקצועיים, זכאים להצטרף על-פי דירוגם המקצועי לאחת מקרנות ההשתלמות בהתאם לבחירתם.
- אחוזי ההפרשה לקרן ההשתלמות הם: 7.5% הפרשת מעביד ועוד 2.5% הפרשת העובד זכאותו של עובד להצטרף לקרן השתלמות תהיה בכפוף לחוקת העבודה לעובדים ברשויות המקומיות.
1. עובד לאחר 12 חודשי עבודה הזכאי לקביעות בהתאם לחוקת העבודה ולהסכמים הקיבוציים. תהא זכאותו להצטרף לקרן השתלמות בתום התקופה.
 2. זכאותו של העובד להצטרף לקרן השתלמות לא תהא מותנית במתן כתב קביעות.
 3. המועד לתשלום יהיה כאמור בסעיף 1 לאחר 12 חודשי עבודה, ולא מעבר לאותה שנת מס.

ממצאים:

- למרבית עובדי הרשות המקומית- קיימת קרן השתלמות כנדרש. כמו כן הפרשות המעביד והעובד לקרן ההשתלמות בהתאם לנהלים.
- נמצא כי **לא קיים מעקב ובקרה אחר מועד זכאותם של העובדים לקבלת קרן השתלמות.**
- במועד ביצוע הביקורת, **נמצאו 12 עובדים שהיו זכאים לקרן השתלמות, וטרם קיבלו את זכאותם.**

נדרש ביצוע בקרה ומעקב אחר זכאותם של עובדי הרשות המקומית לקבלת קרן השתלמות בכפוף לנהלים בנושא.

**כח אדם במוסדות החינוך,
לעומת תקצוב משרד החינוך
מ.מ. יבנאל**

כח אדם קיים במוסדות חינוך - מ.מ. יבנאל, לעומת

תקן/תקצוב משרד החינוך

לבקשת ראש המועצה, בדק מבקר המועצה את תקן כח האדם המועסק בבתי הספר – "נפתלי" ו- "חב"ד" ביבנאל, לעומת תקן/תקצוב משרד החינוך את המוסדות הללו.

ממצאים:

1. כללי השתתפות משרד החינוך:

שירותי היקף - שרתים מזכירים

מערך שירותי העזר כולל שירותי היקף כוללים שאינם שירותי חינוך, אך נחוצים לתפעול שוטף ויעיל של המערכת. במערך שירותי העזר כלולים הנושאים הבאים: **שרתים, מזכירים, סיעות טיפוליות, אבטחת מוסדות חינוך, לבורנטים, ספרנים, עובדי אחזקה, אחראי ציוד ועובדי סיוע.** התשלומים בגין שרתים ומזכירים מבוססים על נתוני התלמידים המדווחים על ידי מנהל בית הספר למטה מצבת תלמידים. **ישנם 2 מודלים לתקצוב נושא זה, פר כיתה או פר תלמיד.** תקצוב פר תלמיד מופעל על כלל בתי הספר הרשמיים. התקצוב פר כיתה מופעל על כלל כיתות החינוך מיוחד. **תקצוב פר כיתה**

תקצוב פר כיתה שרתים (נושא 2)

שיטת ההשתתפות - השרתים מועסקים ע"י הרשויות המקומיות. המשרד מעביר תשלום לפי התבחינים הבאים:
כיתות א' - ו': 4.83 כיתות = 1 משרת שרת
 כיתות ז' - ט': 6.69 כיתות = 1 משרת שרת
 נוסחת החישוב:
 עלות כיתה = עלות משרה לחלק ל 4.83/6.69
 מספר כיתות = לפי כיתות נורמטיביות
 מספר כיתות × עלות כיתה = תשלום

עלות חודשי לשרת במחירי ינואר 2019

עלות משרה:	השתתפות המשרד 87%
₪ 8652.37	₪ 7,527.56

תקצוב פר כיתה מזכירים (נושא 107)

שיטת ההשתתפות - המזכירים מועסקים ע"י הרשויות המקומיות. המשרד מעביר תשלום לפי התבחינים הבאים:
כיתות א' - ח': 15.23 כיתות = 1 משרת מזכיר
 נוסחת החישוב:
 עלות כיתה = עלות משרה לחלק ב 15.23
 מספר כיתות = לפי כיתות נורמטיביות. לפרט את הנוסחה
 מספר כיתות × עלות כיתה = תשלום

עלות חודשי למזכיר במחירי ינואר 2019

עלות משרה:	השתתפות המשרד 87%
₪ 8691.56	₪ 7,561.66

2. תקן משרד החינוך, מול איוש בפועל של כ"א בבתי הספר ביבנאל: שנת הלימודים תש"פ

המוסד החינוכי	סוג המשרה:	תקצוב משרד החינוך	היקף המשרה בפועל	מס' כיתות במוסד החינוכי	סה"כ כיתות	היקף משרה נדרש- בכפוף לתקצוב משרד החינוך	הערות
ביה"ס נפתלי	מזכירה	15.23 כיתות = 1 משרת מזכיר	מזכירה = 0.6 משרה	א-ו = 6 כיתת יער = 1 מונטוסורים = 2	9	0.59	תקין
ביה"ס נפתלי	שרתים + ניקיון	4.83 כיתות = 1 משרת שרת/ניקיון	קבלן ניקיון = 1.1 משרה עובדת ניקיון = 0.86 משרה אב בית = 1 משרה	א-ו = 6 כיתת יער = 1 מונטוסורים = 2	9	1.86	חריגה של 1.1 משרות
			סה"כ: 3 משרות				
ביה"ס חב"ד	מזכירה	15.23 כיתות = 1 משרת מזכיר	מזכירה = 0.8 משרה	א-ח = 8	8	0.53	חריגה של 0.27 משרה
ביה"ס חב"ד	שרתים + ניקיון	א-ו: 4.83 כיתות = 1 משרת שרת/ניקיון ז-ט: 6.69 כיתות = 1 משרת שרת/ניקיון	עובד ניקיון = 0.57 משרה	א-ו = 6 ז-ח = 2	8	1.24	תקין
			אב בית = 1 משרה				
			סה"כ: 1.57 משרות				

3. ביה"ס נפתלי:

3.1. משרת מזכירה:

- בשנת הלימודים תש"פ, מס' הכיתות במוסד החינוכי עמד על 9 {כולל כיתת יער ו-2 כיתות מונטסוריים} - תקצוב משרד החינוך למשרת מזכירה עמד על 0.59 משרה.
- נמצא כי משרת המזכירה בפועל במוסד החינוכי עומדת על 60% - ותואמת את תקן משרד החינוך למוסד החינוכי.

3.2. משרות שרתים {אב בית + ניקיון}:

בשנת הלימודים תש"פ, מס' הכיתות במוסד החינוכי עמד על 9 {כולל כיתת יער ו-2 כיתות מונטסוריים} - תקצוב משרד החינוך למשרת שרת {אב בית + ניקיון}, עמד על 1.86 משרות.

- נמצא כי תקן משרות שרתים {אב בית + עובדי ניקיון} בפועל, עומד על 3

משרות:

- אב בית: 1 משרה
- ניקיון: 0.86 משרה
- קבלן ניקיון: היקף של 1.1 משרה.

- **תקן משרות השרתים בפועל בביה"ס חורג ב- 1.1 משרות מתקן משרד החינוך למוסד החינוכי.**

4. ביה"ס חב"ד:

4.1. משרת מזכירה:

בשנת הלימודים תש"פ, מס' הכיתות במוסד החינוכי עמד על 8 כיתות {א-ח} - תקצוב משרד החינוך למשרת מזכירה עמד על 0.53 משרה.

- נמצא כי משרת המזכירה בפועל במוסד החינוכי עומדת על 80%, קרי: **חריגה של**

0.27 משרה מתקן משרד החינוך למוסד החינוכי.

4.2. משרות שרתים {אב בית + ניקיון}:

בשנת הלימודים תש"פ, מס' הכיתות במוסד החינוכי עמד על 8 כיתות {א-ח} - תקצוב משרד החינוך למשרת שרת {אב בית + ניקיון}, עמד על 1.54 משרות.

- נמצא כי תקן משרות שרתים {אב בית + עובדי ניקיון} בפועל, עומד על 1.57

משרות.

- אב בית: 1 משרה

- ניקיון: 0.57 משרה

- תקן משרות השרתים במוסד החינוכי - תואם את תקן משרד החינוך למוסד זה.

המלצה:

על הרשות המקומית להתאים את תקני המשרות בכל הנוגע לתפקיד מזכירים ושרתים {אב בית + ניקיון}, בבתי הספר היסודיים בתחום הרשות המקומית- לתקן משרד החינוך למוסדות החינוך שנבדקו.

מעקב
אחר תיקון ליקויים
שנים קודמות

מעקב אחר תיקון ליקויים שנים קודמות

<u>נושא:</u>	<u>תיאור הליקוי:</u>	<u>מעקב:</u>
כח אדם ושכר:	נמצא כי המועצה המקומית יבנאל מעסיקה עובדים בתחומים השונים, ללא קבלת נחיצות משרה ו/או פרסום מרכז פומבי לקבלת העובד לעבודה – בניגוד לנהלים ולהוראות קבלת עובדים במועצות המקומיות.	לא תוקן
	<u>עובד המועצה המשמש כקב"ט מוס"ח/רשות – אינו מחויב בשווי רכב צמוד</u> , למרות שהוצמד לו רכב המשמש אותו בכל שעות היממה גם לצרכיו האישיים	תוקן
	הרשות המקומית מעסיקה עובדים בשכר שעתי, ולא בדירוג ודרגה {בכפוף להסכמים הקיבוציים החלים על עובדי הרשויות המקומיות}	תוקן
	ישנם עובדים רבים שסיווג התקציבי בשכרם – אינו תואם את תחום עבודתם. נדרש לפתוח סיווגים חדשים בשכר, ולהעביר עובדים לסיווגים תקציביים קיימים בכפוף לתחום עיסוקם ותפקידם ברשות המקומית.	תוקן חלקית
	עובדים שנתקבלו בשנים האחרונות לעבודה במועצה המקומית יבנאל {במגוון תפקידים} - <u>לא המציאו אישור הקובע את כשירותם הרפואית לעבוד במשרות בהן הם מועסקים</u> .	לא תוקן
תחנת מעבר לפינוי פסולת {מזבלה}:	הפסולת נשארת בתחום השיפוט של המושבה, ללא מתן מענה ראוי לסילוקה כנדרש.	לא תוקן
	הצטברות פסולת וגרוטאות, באתר המזבלה של הרשות המקומית. כתוצאה מהרוח מתפזר חלק מהפסולת בשטח נרחב סביב המזבלה. המקום נראה בכי רע	לא תוקן
	ישנה מכולה המיועדת לפסדים {פגרי בע"ח} - המכולה אינה מתוחזקת כראוי, ואינה מפונה בתדירות הנדרשת. במקום צחנה מחרידה של פסדים {פגרי בע"ח} ואי אפשר היה לעמוד בקרבת המכולה. הריח מתפשט ונישא בכל הסביבה.	לא תוקן
מרכז קהילתי {מתנ"ס} - יבנאל	הרשות המקומית ועמותת המתנ"ס נדרשות להפיק חוזה בין הצדדים, שמטרתו להבטיח את פעולות העמותה בכפוף למטרותיה. החוזה יחתם ע"י 2 הצדדים.	לא תוקן
	הרכב הנהלת המתנ"ס – אינו תואם לתקנון	לא תוקן
	לא נתקבל אישור כשירות המינויים, מאת הוועדה לבדיקת כשירות מינויים בתאגידים עירוניים לנציגי הרשות המקומית בהנהלת המתנ"ס, מקרב עובדי המועצה ומקרב הציבור	לא תוקן
כלי רכב מועצה: הוצ' דלק וסולר	למעט רכב ראש המועצה – לא קיימים התקני תדלוק אוטומטיים ברכבי המועצה.	לא תוקן
	המשתמשים בכלי הרכב במועצה - אינם מנהלים ספר רכב. לא קיימים נוהלי עבודה מסודרים ומחייבים בנוגע לשימוש ברכבי המועצה.	לא תוקן
	הוצאות בגין רכישות בנזין וסולר - עבור כלי העבודה יירשמו בנפרד למחלקת המשק ובנפרד למחלקת הגינון	לא תוקן

המשך- מעקב אחר תיקון ליקויים קודמים:

נושא:	תיאור הליקוי:	מעקב:
אינוונטר { ניהול מצאי }:	- ניהול האינוונטר אינו ממוחשב - אינו מנוהל באמצעות תוכנה ייעודית. - המועצה אינה מקפידה להטביע על ציוד המצאי, את סמל הרשות המקומית. - לא ניתן לציוד מספר סידורי.	לא תוקן
גריעת מצאי:	- גריעת פריטים ממצאי המועצה כמעט ולא נעשית. - ועדת רכש ובלאי- אינה מתכנסת לדון בגריעת מצאי עקב-התיישנות הציוד, אובדן ציוד, ציוד לא תקין.	לא תוקן
רישוי עסקים:	עסקים רבים פועלים ללא רישוי.	לא תוקן
	הרשות המקומית לא מבצעת אכיפה – אין הוצאת צווי סגירה.	לא תוקן
	הרשות המקומית טרם השלימה את עריכת המפרט הרשתי. כמו כן טרם פרסמה את הדרישות באתר האינטרנט של הרשות המקומית.	לא תוקן
	טרם מונה גורם מוסמך ברשות המקומית לקבלת ההשגות. ולא פורסם באתר האינטרנט של המועצה, פרטים בדבר הגשת ההשגה	לא תוקן
	טרם הוקמה עמדת עיון	לא תוקן
