לשכת מבקר העירייה
והממונה על תלונות הציבור

# דוח ביקורת

# בנושא אבטחת מידע

# דוח ביקורת בנושא אבטחת מידע

## 1. מבוא

### 1.1. כללי

בשנים האחרונות, אבטחת מידע הפכה צורך בסיסי לכל ארגון באשר הוא.

פגיעה בחיסיון המידע, עלולה לגרום לארגון עצמו ולגורמים שונים שפרטיהם כלולים במאגרי המידע שלו לנזקים משמעותיים.

מטרת אבטחת המידע הינה הגנת המידע (לרבות סודיות, אמינות, וזמינות) מפני פגיעה מכוונת או מקרית, או ניצולו לרעה.

להשגת מטרה זו, אבטחת המידע תפעיל בקרות פנימיות וחסמים בתוך מערכות המידע.

אבטחת מידע היא מכלול האמצעים במערכת ובארגון שתפקידם להבטיח שהמידע האגור במערכת מוגן וממודר .

אבטחת מערכות מידע מחייבת ניהול מתמיד של קונפליקט מובנה בין הצורך לאפשר נגישות ושימוש מרבי במערכות המידע לבין הצורך להגן עליהן. השגת האיזון הנכון תוך בקרה נאותה מציבה אתגר משמעותי לפני כל ארגון.

ככל שהזמן חולף, מתבסס המחשב ככלי עבודה אלמנטרי המשמש למרב הפעילויות הכרוכות בעיבוד מידע. רשתות תקשורת מקשרות בין מחשבים בתוך הרשות ומחוצה לה. רשתות חיצוניות, כגון: רשת האינטרנט, אשר הפכה לנפוצה ביותר, מאפשרת נגישות מהירה וקלה למידע רב.

השימוש בדואר האלקטרוני החליף את אמצעי התקשורת הקלאסיים.

יחד עם ההזדמנויות והיתרונות שנוצרו מקלות הקישוריות וזמינות המידע, נוצרה בעיה קשה של אבטחת מידע.

כמו מרבית הארגונים גם עיריית הוד השרון חשופה היום, יותר מאי פעם, לנסיונות ולאיומי חדירה למאגרי המידע שלה ולהתקפה על המידע המועבר באמצעות רשתות התקשורת.

על מנת ליצור תשתית אבטחת מידע אמינה במערכות המידע והתקשוב, יש ליצור מודעות לסוגיית האבטחה, לבסס ידע עדכני לעניין אבטחה זו, וכמובן ליישם ולאכוף את האמצעים לאבטחת המידע במערכות השונות.

### 1.2. האחריות לניהול אבטחת המידע בעיריית הוד השרון

האגף למערכות מידע בעירייה (להלן: "האגף") אחראי לניהול אבטחת המידע בעירייה.

נכלל בכך ניהול מאגרי המידע בעיריה בהם מצויים נתונים רבים ומגוונים, כולל פרטים אישיים, על תושבים, עובדי עירייה וגורמים נוספים (כמו יזמים לסוגיהם).

1.3. **מטרת הביקורת**

מטרת הביקורת הינה לבדוק את אופן הפעילות והתפקוד של האגף בנושא אבטחת המידע, על מיגוון הפעילויות הכלולות בכך, להצביע על ליקויים, אם יימצאו ולהמליץ על דרכים לתיקונם.

1.4. **תקופת התייחסות הביקורת**

הביקורת מתמקדת בעיקר בשנים 2019 עד 2021.

1.5. **תפקוד האגף**

ככלל, הביקורת מצאה ניהול תקין ותפקוד מניח את הדעת של האגף בנושא הביקורת. עם זאת נמצאו בביקורת ליקויים, פערים וחריגים כמפורט להלן בסעיפי הדוח השונים.

1.6. **סיוע לביצוע הביקורת**

הביקורת מודה למנהלת האגף ולצוותה על הסיוע בעריכת ביקורת זו, הן בהמצאת נתונים וחומרים והן במענה לשאלות הביקורת.

# 2. בסיס חוקי - נורמטיבי

הבסיס החוקי או הנורמטיבי לנושא אבטחת מידע:

2.1. חוק הגנת הפרטיות התשמ"א 1981.

2.2. תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

2.3. תקן ISO 27001. (נורמטיבי אבל לא מחייב מבחינת החוק)

# 3. נוהלי עבודה

3.1. **כללי**

לבקשתה, הביקורת קיבלה מהאגף תיקיית קבצים גדושת מסמכי נהלים – בסה"כ **80 נהלים** !! מתוכם כ-50 נהלים הינם בפורמט מיושן והינם עיבוד של מסמכי נוהל שמקורם (למיטב הזיהוי של הביקורת) בשנת 2010 (מעל ל- 10 שנים). יצוין כי על הנהלים עצמם או על שמות הקבצים שלהם אין תאריך.

אלו יקראו כאן **"קבוצת נהלים א'"** דוגמת נוהל בנספח א'

כ- 5 עד 10 נהלים הינם משנת 2007, - להלן **"קבוצת נהלים ב"**. דוגמת נוהל בנספח ב'.

כ- 15 עד כ-20 נהלים הינם מהשנים 2018 ו- 2019. להלן **"קבוצת נהלים ג' "** . דוגמת נוהל בנספח ג'.

3.2. **ממצאים והתייחסות הביקורת**

**3.2.1 כמות הנהלים ומידת השימוש העכשווי בהם**

לפי כמות הנהלים "הבלתי קונונציונלית" בתיקיית הנהלים שנתקבלה בביקורת והשונות הרבה במאפייני הנהלים (כמו מועד ההכנה, פורמט המסמך, מספור המסמך ועוד), הביקורת מגיעה למסקנה כי חלק ניכר מתוך הנהלים האלו איננו בשימוש ואף איננו מתאים היום לתהליך / תהליכים אשר הנוהל אמור להוות מתווה לביצועו / ביצועם.

מסקנה זו של הביקורת נסמכת גם על היעדר רישום של מועד הכנת הנוהל, מועד תוקף הנוהל ומועד פגות תוקף של כל נוהל.

עפ"י המסקנות לעיל, הביקורת ממליצה לבצע סקירה מקצועית של כלל הנהלים בתיקיה ועל בסיס סקירה זו לבצע פעילות של ארגון הנהלים לרבות:

(1) מיפוי (מקצועי, אובייקטיבי ובלתי תלוי) של התהליכים השונים הנדרשים בנושא אבטחת מידע בעיריית הוד השרון. מיפוי זה צריך לשמש כמפת דרכים וכמיתווה מנחה ומחייב לעניין הנהלים. אל מול מיפוי זה:
(2) סינון וגניזת כל מסמכי הנוהל שכבר אינם אקטואליים או בכפילות (או דומים ) עם מסמכים אחרים
(3) הותרה וריכוז רק של הנהלים שהינם מתאימים והולמים לתהליכים הנוכחיים באגף בנושא אבטחת מידע
(4) הכנת רשימה של נהלים חסרים ו/או דורשים תיקון / הסבה / התאמה לצורך העכשווי.

**3.2.2 פורמט הנהלים**

בכל קבוצת נהלים, כמצוין לעיל, פורמט מסמך הנוהל שונה כפי שניתן לראות בנספחים הנ"ל. השוני מתבטא ב:

3.2.2.1 מספר מזהה לנוהל

בקבוצה א' – יש מספר מזהה לכל נוהל. בקבוצות ב' ו- ג' אין. לתפיסת הביקורת שוני זה באוסף הנהלים לאותו נושא בתוך יחידה ארגונית אחת **מהווה ליקוי**. כמו כן היעדר מספר מזהה, חד ערכי, במסמך נוהל שאמור להיות מסמך מבוקר, **מהווה ליקוי מהותי.**

3.2.2.2 כותרת עליונה לכל עמוד במסמך הנוהל:

נמצא כי כותרות מסמך (עליונות) שונות לנהלים שונים במספר נוסחי כותרת. לפירוט ראה נספח ד'.

3.2.2.3 כותרת תחתונה מובנית בכל עמוד

נמצא כי כותרת מסמך תחתונה מובנית, יש רק בנוהלי קבוצה א'. לפירוט ראה נספח ה'.

**3.2.3 מיתווה הנושאים בנוהל**

בקבוצה א' של הנהלים מיתווה הנושאים בנוהל אחיד וחוזר בכל נוהל ונוהל. לפירוט המתווה בקבוצה זו ראה בנספח ה' לעיל. בקבוצות הנהלים האחרות אין מתווה אחיד ובחלקן אין כל סדר נושאים. לעיתים הנוהל כמכתב, לעיתים כסיכום דיון, לעיתים כנייר עמדה ( מדיניות אבטחת מידע בקובץ הנהלים וכו').

**3.2.4 התייחסות הביקורת**

לתפיסת הביקורת ערב רב זה של פורמטים לנהלים בפרמטרים השונים כפי שפורט, מהווה פגם מהותי בניהול נושא הנהלים ובנושא הנדון "אבטחת מידע" אופן זה של פורמט נהלים מהווה ליקוי מהותי ואף חמור ואיננו תקין.

3.3. **תאריכים**

אין בחלק ניכר מהנהלים כל תאריך או מועד מוגדר. זאת לא למועד ההקמה, הכתיבה, אישור הנוהל וכו'. יש להדגיש כי נוהל הינו ככלל מסמך מבוקר (וקל וחומר בנושא אבטחת מידע בעירייה).

לתפיסת הביקורת, היעדר תאריכים ומועדים במסמכי הנהלים מהווה ליקוי מהותי.

3.4. **צורת ההנחיות והדרישות לביצוע בנהלים**

**3.2.5 מה נכון וצריך, לתפיסת הביקורת ומה יש בפועל**

3.2.5.1 קביעת ממלאי תפקיד ליישום הנחיות

ההנחיות והדרישות לביצוע בנהלים צריכים להיות בהירים, חדים, ומיוחסים לממלא תפקיד או ממלאי תפקידים מוגדרים. הנחיות בדרך זו קיימות בחלק מהנהלים **ובחלק ניכר מהנהלים אינן קיימות.** יש בכך ליקוי מהותי.

3.2.5.2 מועדים

נדרשת קביעה של לוחות זמנים, מועדים ו/או קביעת מועדי מקסימום או משך טיפול תקין. ברוב הנהלים אין קביעות והגדרות כאלו. היעדרם מהווה ליקוי מהותי.

3.2.5.3 אנומליות וכשלים

נדרשת התייחסות בנהלים ומיתווה מנחה לביצוע במקרה של אנומליות בתהליך ו/או כשלים.

במרבית הנהלים אין התייחסות למצבים כאלו. היעדרם מהווה ליקוי מהותי.

3.2.5.4 טבלאות ותרשימי תהליך

כדי לעשות את הנהלים לברורים, חדים, ומספקים התוויה ליישום תהליכים, נדרש להוסיף או לשתול בנהלים טבלאות ו/או תרשימי תהליך ליישום הנוהל בצירוף הגדרת אחראיים ומבצעים וכיו"ב.

אין בנהלים ביטוי לדרישה זו. היעדרם מהווה ליקוי מהותי.

3.5. **מסקנות והמלצות**

מתוך הממצאים לעיל, הביקורת מגיעה למסקנה כי הנהלים לנושא אבטחת מידע אינם מנוהלים ומופעלים באופן תקין, המתאים לחשיבותם ערכם של נהלים בנושא זה. לתפיסת הביקורת, נושא של אבטחת מידע ברשות מקומית כמו עיריית הוד השרון (עם השלכות לכ-65 אלף איש) **מחייב** נהלים איכותיים, עדכניים ומעשיים ברמה הגבוהה ביותר.

**למסקנת הביקורת** היעדרם של נהלים איכותיים ביותר בנושא האמור, יוצר חשיפות לסיכונים משמעותיים בעלי פוטנציאל נזק חמור.

**הביקורת ממליצה** לפעול בהקדם רב לשיפור ולתיקון כל הליקויים והפגמים שצוינו לעיל

3.6. **ממצאי – דוח סטטוס אבטחת מידע מ-08/08/2020**

בדוח סטאטוס אבטחת מידע שנערך ע"י ר.א. - מנהל מידע אשכול רשויות השרון נכתב בנושא זה:

נהלים: **מבדיקה עולה כי אין בעירייה נהלי אבטחת מידע מאושרים** , הועברו סט נהלים (נוהל שימוש במצלמות , נוהל גישה של נותן שירות חיצוני לרשת, נוהל הוראות הגנת מידע , נוהל שינויים , נוהל אחראיות עובדים) לאישור העירייה. קיים **העדר מנגנון ארגוני לניהול אבטחת מידע** .

התייחסות הביקורת: מימצאים אלו מצטרפים לממצאי הביקורת, מאששים את מסקנותיה לעיל ותומכים בהמלצותיה.

3.7. **תגובת האגף לטיוטת דוח הביקורת והתייחסות הביקורת**

3.7.1. **תגובת האגף**

רשות מקומית מחויבת לחוק הגנת הפרטיות ותקנותיו (תשמ"א) ותו לא.
אין כל בסיס חוקי אחר בהיבטי אבט"מ המחייב רשות מקומית לנהלי עבודה כך שכל נהל עבודה תפעולי הינו בגדר המלצה בלבד (ללא כל חבות), למעט נוהל מאגר מידע (נדרש מתוקף החוק ותקנות הגנת הפרטיות), אשר נמצא בהתהוות בימים אלו.
באשר לנהלי עבודה תפעוליים, בכוונתנו לכתוב מספר מצומצם של נהלים (המהותיים לתפעול השוטף של האגף) ע"מ לשקף את תהליכי העבודה בפועל וייצר תהליך סדור.

3.7.2. **התייחסות הביקורת**

הביקורת בדקה את נושא הנהלים ככלי ניהולי שיכול לסייע לניהול ולביצוע תהליכי האגף הנוגעים לאבטחת מידע ולא עקב חבות עמידה בדרישות חוק כזה או אחר.
מבחינת הביקורת, בחירת האגף להתמקד בנהלים מהותיים לתפעול תהליכי העבודה, מקובלת כל עוד הדברים מיושמים עפ"י החלטה סדורה ועל בסיס חשיבה ותכנון.
הביקורת מממליצה ליישם הלכה למעשה את הכוונות המתוארות בתגובת האגף ובזמן קצר.

# 4. מדיניות אבטחת מידע

4.1. **כללי**

בקובץ נהלי אבטחת מידע, ישנו מסמך "מדיניות אבטחת מידע ונהלים" מתאריך 10/3/2019 וחתומים עליו המנכ"לית הקודמת - חנה גולן, והמנמ"רית הקודמת – אירית הכהן.
למסמך ראה נספח: ז'
עצם קיומו של מסמך מדיניות אבטחת מידע באגף מערכות מידע ראוי לציון חיובי.

4.2. **נושאי המסמך**

הביקורת מתרשמת כי המסמך מקיף וכולל את מרבית הנושאים וההיבטים הנדרשים במסמך מדיניות אבטחת מידע

4.3. **תאימות לעיריית הוד השרון**

על אף שהמסמך, כאמור בסעיף 5.2 לעיל כולל את כלל הנושאים והם "מכסים" מן הסתם את הדרישות לאבטחת מידע בהוד השרון, אין במסמך כל התייחסות למאפיינים ולצרכים ייחודיים ומיוחדים של הוד השרון.
למיטב הבנת הביקורת המסמך הינו מסמך גנרי למסמך מדיניות אבטחת מידע שהועלו עליו כותרות של עיריית הוד השרון.
לתפיסת הביקורת, היעדר כל מאפיין ייחודי וספציפי להוד השרון במסמך מהווה פגם מהותי.

4.4. **עדכנות**

לתפיסת הביקורת, ניהול אבטחת מידע (והגנת סייבר) הינו כה דינמי ועתיר שינויים מהירים, תכופים ורציפים, שחייב להיגזר מכך מענה דינמי גם במסמך המדיניות לנושא. לפיכך, לתפיסת הביקורת היה ראוי כי מסמך זה יעבור ריענון ועדכון לפחות פעם בשנה. המסמך שלפנינו נושא תאריך של תחילת 2019 ומאז " מים רבים זרמו בנהרות הסייבר" ולפיכך היה ראוי לעדכנו ולהתאימו. (כאמור גם להוסיף בו מאפיינים וייחוד של עיריית הוד השרון).

4.5. **ניהול מדיניות אבטחת המידע**

לתפיסת הביקורת מדיניות האיכות אמורה להוות כתוכנית אסטרטגית של העירייה ביחס לנושא אבטחת המידע. לתפיסת הביקורת, על תוכנית כזו כמו על כל תוכנית אסטרטגית בארגון להיות מנוהלת באופן ממוקד ולאורך זמן וזאת בהיבטים שעיקרם:

**4.5.1 מחויבות של הנהלת הארגון ( אגף מערכות מידע והנהלת העירייה) למדיניות**

נכללים במחויבות זו:

4.5.1.1 "כיסוי" הנושא במשאבים הראויים - אמצעים, כ"א, תקציב הולם.

4.5.1.2 ניהול הנושא ברמה הניהולית (מעורבות בנושא לפחות ברמה של צוות היגוי פעיל).

4.5.2 **תוכנית יישום להשגת מטרות ויעדי המדיניות.**

נדרש כי כנספח / נספחים למסמך המדיניות יוכן מסמך תוכנית יישום כולל:

4.5.2.1 הגדרת מטרות.

4.5.2.2 הגדרת קריטריונים ומדדים שעל פיהם ימדדו יישום התוכנית.

4.5.2.3 תמונת מצב על "סרגל" כמותי ככל הניתן של אותם קריטריונים ומדדים בנקודת המוצא של התוכנית.

4.5.2.4 קביעת יעדים כמותיים על ציר הזמן לשיפור / העלאה / שידרוג של קריטריונים ומדדים אלו.

**<u>לתפיסת הביקורת</u>** נדרש מעת לעת ובנושא דינאמי זה שאנו עוסקים בו, **<u>לפחות אחת לשנתיים</u>** עדכון וריענון של התוכנית האסטרטגית לאמור מסמך מדיניות ניהול אבטחת המידע של העירייה.

**<u>להבנת הביקורת</u>**, מתוך החומרים שנמסרו לה כל האמור בסעיף זה (סעיף 4.5) לא קיים היום באגף מערכות המידע.

**<u>לתפיסת הביקורת</u>** היעדרם של כל אלו מהווה פער בלתי רצוי ופגם בנושא מדיניות אבטחת המידע. הביקורת ממליצה לפעול להשלמת הנ"ל בהתאם.

4.6. **ממצאי - דוח סטטוס אבטחת מידע מ-08/08/2020**

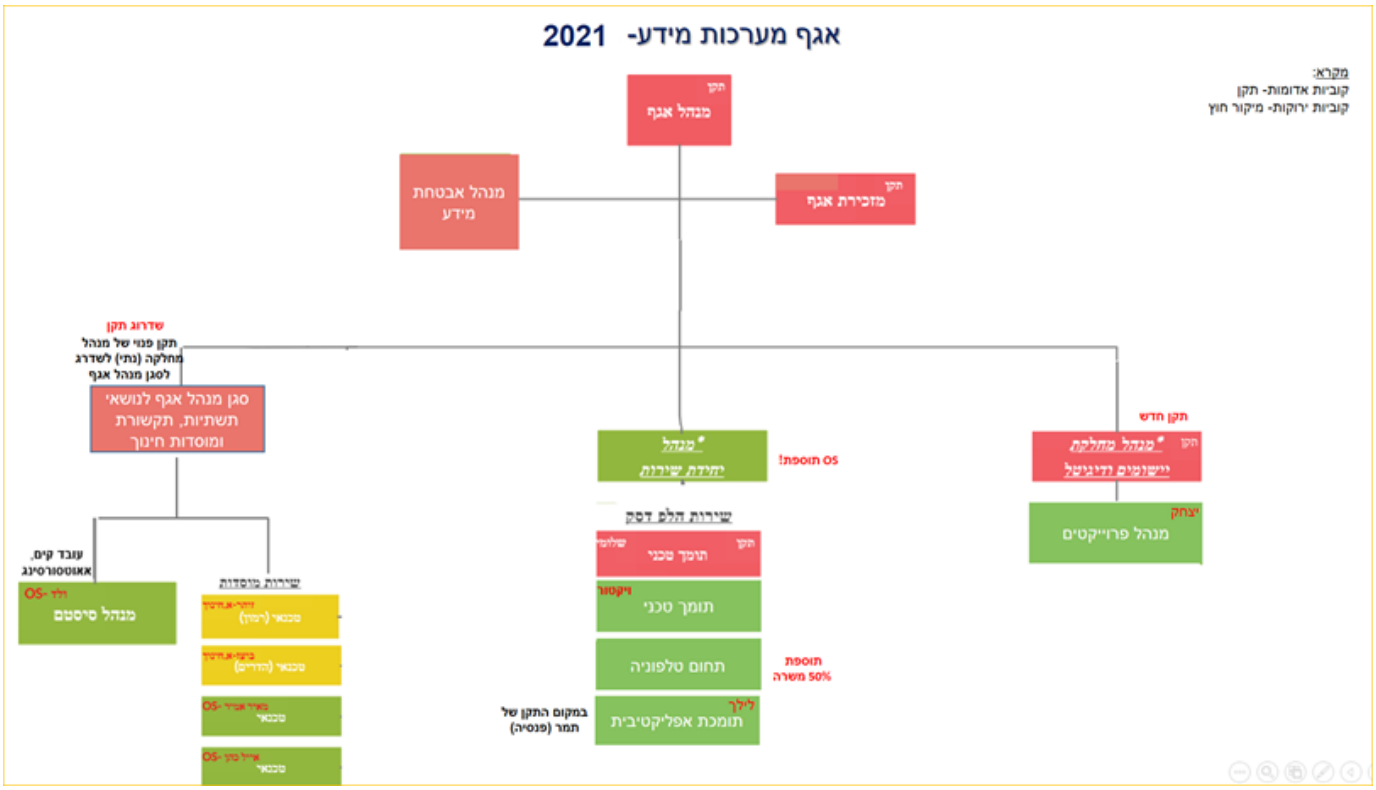
בדוח סטאטוס שנערך ע"י ר.א. - מנהל מידע אשכול רשויות השרון נכתב בנושא זה :

מסמך מדיניות אבטחת מידע – "נדרש לתקף על פי חוק את המסמך אחת לשנה – הועבר נוסח מעודכן לחתימה." הביקורת רואה בחיוב קיום דרישה זו, ולכאורה מהווה (אמנם באיחור) יישום המלצתה מסעיף 4.4 לעיל.

יצוין כי הכתוב ע"י מנהל מידע אשכול רשויות השרון בדבר מחויבות חוקית למסמך מדיניות איננה נכונה.

# 5. המערך הארגוני

## 5.1. תרשים המבנה הארגוני




## 5.2. התייחסות הביקורת לתרשים המבנה הארגוני

בתרשים המבנה הארגני מוצגת יחידת אבטחת מידע. עצם קיום יחידה כזו במבנה הארגוני של האגף בכפיפות ישירה למנהלת האגף אומר דרשני לחיוב וראוי לציין זאת כך.

עם זאת, מהתרשים עולה כי:

5.2.1. מדובר במנהל אחד בלבד ללא כל צוות. לדעת הביקורת, צורכי הניהול והפעילות הנגזרים מהיקף הנושאים, מערכות המידע ומאגרי המידע בעירייה מחייבים צוות גדול יותר מאדם אחד.

5.2.2. מנהל אבטחת מידע מוצג כפונקציה מסייעת / מייעצת למנהלת האגף ללא כל קשרים ישירים אופרטיביים עם הפונקציות האחרות באגף או "בשטח".

5.2.3. מתוך התרשים לא ניתן ללמוד את דרך הפעילות והשירות של יחידת אבטחת המידע.

5.2.4. נדרש וחיוני להוסיף לתרשים הגדרה ותיאור תפקיד ( כולל תחומי אחריות, תהליכים ופעילות וכו' ) של מנהל אבטחת המידע. (וצוות, כאמור)

5.2.5. לא מוצגת בתרשים הפונקציה של ממונה אבטחת מידע (ראה בסעיף 6. להלן).
היעדר פונקציה זו מהווה פגם בתרשים המבנה.

5.3. **האגף באתר העירייה**

לממצא הביקורת, נכון ליול 2021 , האגף למערכות מידע איננו מופיע כלל באתר האינטרנט, ברשימת יחידות העירייה.

לראיית הביקורת היעדר כל איזכור וסימן לאגף באתר העירייה מהווה ליקוי מהותי.

# 6. ממונה אבטחת מידע במאגר/י המידע

6.1. **מינוי ממונה**

עפ"י תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז – 2017, מונה ע"י מנכ"ל העירייה ב-19/5/2021 ממונה אבטחת מידע בכל מאגרי המידע המוחזקים ע"י העירייה. לכתב המינוי ראה נספח ח'.

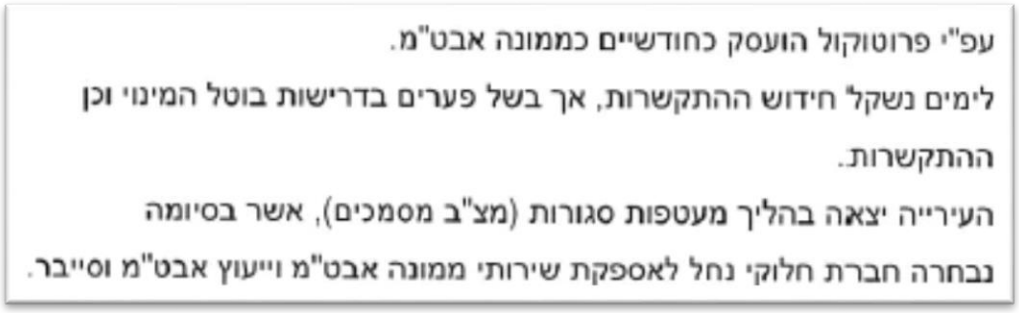
מסקנת הביקורת: המינוי תקין.

6.1.1. ביטול המינוי

הנתונים על המינוי נמסרו לביקורת במהלך אוגוסט 2021. לקראת סוף שנת 2021 הסתבר לביקורת כי בפועל התפקיד איננו מאויש וכי המידע שנמסר לביקורת לא היה מדויק ועדכני ואכן בתגובת האגף לטיוטת דוח הביקורת מסתבר כי ממונה אבט"מ הועסק רק כחודשיים והמינוי שלו בוטל. לא מצוינים בתגובת האגף מתי מתחילה תקופת ה"כחודשיים" ומתי היא מסתיימת.

6.1.2. בחירת ממונה אבט"מ אחר

עפ"י תגובת האגף לטיוטת דוח הביקורת:




מתוך תגובת האגף לטיוטת דוח הביקורת, הביקורת למדה כי האגף בחר בספק חיצוני אחר לספק את שירותי אבט"מ. להערכת הביקורת בחירה זו נעשתה, כנראה, לקראת סוף 2021. (האגף לא צירף לביקורת מסמכים על הליך הבחירה – למרות שבתגובתו כתב "מצ"ב מסמכים". כמו כן בתגובת האגף לטיוטת הדוח לא מוצג אפילו תאריך אחד).

6.2. **הגדרת תפקיד – להתקשרות ממאי 2021**

הוגדר תפקידו של ממונה אבטחת המידע. ראה נספח ט' . לדעת הביקורת, במסמך הגדרת התפקיד **<u>ליקויים מהותיים</u>** שעיקרם:

6.2.1. המסמך לא נושא כל סימנים שמדובר בעיריית הוד השרון או באגף למערכות מידע.

6.2.2. אין על המסמך תאריך.

6.2.3. מצוין במסמך כי ממונה אבטחת המידע עובד בשוטף עם מנמ"רית העירייה ועם מנהל אבטחת המידע. אין כל פירוט נוסף על מה הוא עובד באיזה נושאים.

6.2.4. אין הגדרה ואין נוהל כיצד מתחלקת תכולת העסקתו בין ההתעסקות בתחומי האחריות הנוגעים לתפקידו כממונה לבין יתר עיסוקיו.

6.2.5. כתוב במסך כי יש אצלו עובד צמוד "מטעמו" המסייע לו בביצוע תפקידו. במקרה זה של עובד צמוד המסייע לו בביצוע תפקידו, היה ראוי כי יפורטו תחומי האחריות של אותו עובד צמוד.

6.2.6. כתוב במסמך כי יש לו תפקידים נוספים : ייעוץ שוטף (טכנולוגי וארגוני). לראיית הביקורת נדרש וחיוני פירוט נוסף של אותם תפקידים נוספים. היעדר פירוט כזה מהווה ליקוי. ראוי להדגיש כי הגדרת תפקיד - לא אמורה להיות מכוונת לאדם מסוים אלא לפונקציה התפקודית.

**<u>לסיכום: למסקנת הביקורת</u>** במסמך הגדרת התפקיד של הממונה ובתכנים בו, הביקורת מצאה ליקויים, חלקם מהותיים. **הביקורת ממליצה** לתקן ליקויים אלו בהקדם.

6.3. **ממונה אבטחת מידע בהתקשרות קבלנית - להתקשרות ממאי 2021**

6.3.1. <u>מסמכי התקשרות - הסכם</u>

מתוך הגדרת תפקיד ממונה אבטחת המידע, כמפורט בסעיף הקודם (6.2), ניתן להבין כי הממונה הינו ספק חיצוני / קבלן בהתקשרות חוזית.

באגף פתרו את נושא **<u>ממונה</u>** אבטחת המידע במאגרי המידע של העירייה ע"י התקשרות חוזית עם איגוד ערים "אשכול רשויות השרון" (להלן "האיגוד"). עפ"י הצעת מחיר של האיגוד (נספח י'), האיגוד מעמיד לרשות עיריית הוד השרון, עובד שישמש כ**<u>מנהל</u>** אבטחת מידע, בהיקף משרה של 15 שעות שבועיות, כ-35% משרה (בעלות חודשית של 12,500 ₪). יצוין כי בה בעת פעל באגף ממלא תפקיד שכיר (במשרה שלמה) כמנהל אבטחת מידע כפי שמוצג בתרשים המבנה הארגוני בסעיף 5.1 לעיל.בין הגדרת התפקיד של מנהל אבטחת המידע **<u>עפ"י הצעת האיגוד</u>** כלולים גם, תפקידי **<u>ממונה</u>** אבטחת מידע למאגרי העירייה. (כנדרש עפ"י חוק ותקנות) כמו "בניית תוכנית עבודה שנתית", "מילוי טפסים ובקשות בכל הקשור לניהול מאגרי המידע מול משרד המשפטים", "שליחת עדכונים לעובדים בתחום אבטחת מידע".

יצוין כי דרישת החוק והתקנות להגנת הפרטיות מגדירה **"ממונה"** על אבטחת מידע ואין בהם כל איזכור או התייחסות ל- **"מנהל"** אבטחת מידע. עם זאת מ- "תקנות אבטחת הפרטיות (אבטחת מידע)" ברור כי ממונה אבטחת מידע יכול לעסוק בעיסוקים נוספים ובלבד שלא יעמדו בניגוד עניינים. " (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; "

6.3.2. <u>היקף המשרה</u>

כאמור, נשכר עובד חיצוני לתפקיד מנהל אבטחת מידע (ובתוך זה תפקידי ממונה אבטחת מידע) בהיקף מצומצם של 15 שעות לשבוע. ( כ-35% משרה).

לא הומצא לביקורת כל תיעוד לביסוס היקף זה. שיעור זה של היקף משרה מעלה תמיהה לאור מכרז למשרת מנהל אבטחת מידע באגף מערכת מידע (מכרז פומבי 135/17 - נספח י"א) שנוהל ע"י אגף משאבי אנוש בעירייה. בדצמבר 2017. לגבי היקף המשרה כתוב במכרז:

היקף המשרה: מסלול קידום של מנהל מחלקה ברשות מקומית רמה בי בדרוג הטכנאים וההנדסאים 39-41 או דרוג מחי"ר בהתאם לכללים הנהוגים בשרות בציבורי או העסקה בחוזה אישי בכפוף לאישור משרד הפנים

למרות שלא מצוין במפורש כי המדובר במשרה מלאה, הביקורת מבינה מהכתוב כי אכן הכוונה למשרה מלאה.

הביקורת תמהה כיצד, במציאות של סיכוני ואיומי סייבר גוברים והולכים לרבות אירוע חדירה משמעותי שהיה לאחרונה בעירייה, החליטה הנהלת אגף מערכות המידע על הנחתת המשרה הזו מ- 100% ב-2017 ל-35% בלבד ב- 2020/21 .

הסימוכין היחיד להיקף המשרה האמור (35%) מצוי בהצעה מאת מנמ"ר אשכול רשויות השרון (נספח י'):

לדעת הביקורת אין בסימוכין זה להוות ביסוס מנומק להיקף זה של משרה.

לתפיסת הביקורת, לנוכח המובא לעיל, היעדר ביסוס והנמקה להנחתה זו מהווה, ליקוי בהתנהלות ודורשת בדיקה ובחינה להצדקתה. הביקורת ממליצה לערוך בדיקה כזו בהקדם.

6.3.3. <u>תיחור / התמחרות</u>

6.3.3.1. <u>התקשרות ללא מכרז וללא תיחור</u>

ההתקשרות למנהל אבטחת מידע נערכה עפ"י אישור של וועדת שלושה מיום 5.5.2020 בהרכב הכולל את המנכ"ל, היועמ"ש, הגזבר ובהשתתפות המנמ"רית, מנהל וסגן מנהל מח' חוזים ומכרזים. ההתקשרות נעשתה ללא מכרז והסתמכה על ציטוט שהמנמ"רית העלתה בדיון כדלקמן:

<u>אילן מעדכנת</u>:
בהתאם לתקנות העיריות מכרזים, רשות מקומית רשאית להתקשר עם האשכול אשר הינו איגוד ערים, בפטור ממכרז, לקבלת שירותים מהסוג שניתן על ידי האשכול, במסגרת סמכויותיה ותפקידיה לפי כל דין, לצורך מילוי סמכויות העירייה ותפקידיה.
לפיכך ולאור צרכים דחופים ופערים שקיימים בתחום, אנו מבקשים להתקשר עם האשכול לצורך קבלת שירותי מנהל אבטחת מידע במסגרת הסכם למתן שירותי מנמ"ריה עם האשכול.
השירות כולל 15 שעות שבועיות הכוללות ניהל ובקרה של מערך אבטחת המידע בעירייה, בניית תכנית עבודה שנתית ומעקב אחר ביצוע באופן שוטף, מילוי טפסים ובקשות בכל הקשור לאבטחת מידע וניהול מאגרי המידע מול משרד המשפטים, שליחת עדכונים לכלל עובדי העירייה בתחום אבטחת מידע, ביצוע בדיקות פתע וחדירות לתשתיות המחשוב.

התייחסות הלשכה המשפטית לסוגיית הפטור ממכרז ולוויתור על תיחור

ב- 3/5/2020 כותבת אל המנמ"רית עו"ד ל.ג. ,סגנית יועמ"ש העירייה" כדלקמן:

בהתאם להוראות סעיף 3(16) לתקנות העיריות (מכרזים), ניתן להתקשר בפטור ממכרז במידה ומדובר ב"התקשרות עם רשות מקומית אחרת לקבלת שירותים מהסוג שניתן על ידה במסגרת סמכויותיה ותפקידיה לפי כל דין, לצורך מילוי סמכויות העירייה ותפקידיה לפי כל דין, לאחר שהעירייה שוכנעה שההתקשרות נדרשת מטעמי חיסכון ויעילות והיא מיטיבה עם העירייה".

בהתאם לאמור בהוראות סעיף 3(16) לתקנות המכרזים - יש להביא את ההתקשרות עם האשכול לאישור ועדת ההתקשרויות על מנת שתאשר כי ההתקשרות עם האשכול עונה על הקריטריונים המפורטים בתקנה 3(16) ובעיקר כי "העיריה שוכנעה שההתקשרות נדרשת מטעמי חיסון ויעילות והיא מיטיבה עם העיריה". לשם כך עלייך להמציא המלצה לוועדת ההתקשרויות כי מדובר בהתקשרות העונה על הקריטריונים המוגדרים בסעיף הנ"ל, לאחר שבחנת אפשרויות שונות להתקשרות בעניינים אלה ועל הגזברות להמציא אישור כי ההתקשרות עם האשכול תהווה חסכון כספי לעיריה לעומת אפשרויות אחרות.

6.3.3.2. <u>היעדר תיעוד על בחינת חלופות הולמות להתקשרות במיקוד לחסכון מירבי בעלויות</u>

לביקורת לא הומצא כל תיעוד על בחינת חלופות נוספות להתקשרות שנערכה עם האיגוד או לתהליך תיחור כזה או אחר על הצעות אחרות להספקת השירות הנדרש. וזאת בהלימה להנחיות החוקיות של סגנית היועמ"ש.

מכאן, הביקורת מגיעה למסקנה כי ,לכאורה, לא היה תיחור כזה ולא היתה בחינת חלופות להצעת האשכול. הביקורת מוצאת היעדר הליך בדיקת חלופות, כאמור, ותהליך תיחור בין מספר הצעות, ליקוי מהותי והתנהלות בניגוד לאמור בהוראות סעיף 3 (16) לתקנות המכרזים.

6.3.4. <u>אי חוקיות, לכאורה, של ההתקשרות ללא מכרז עם האיגוד</u>

6.3.4.1. <u>ציות לתקנות העיריות</u>

בטרם התכנסות וועדת השלושה (ב-5/5/2020), ב- 3/5/2020 סגנית היועמ"ש של העירייה ניסחה את התנאים לאפשרות התקשרות ללא מכרז עם האיגוד כדלקמן:

**From:** ליה גרנות<LiaG@hod-hasharon.muni.il>
**Sent:** Sunday, May 3, 2020 11:19 AM
**To:** אילן כהן<IlanC@hod-hasharon.muni.il>
**Cc:** אבידע שדה<AvidaS@hod-hasharon.muni.il>
**Subject:** RE: מנמריה אזורית אשכול השרון/הוד השרון + מנהל אבטחת מידע אזורי

אילן שלום,

בהתאם להוראות סעיף 3(16) לתקנות העיריות (מכרזים), ניתן להתקשר בפטור ממכרז במידה ומדובר ב"התקשרות עם רשות מקומית אחרת לקבלת שירותים מהסוג שניתן על ידה במסגרת סמכויותיה ותפקידיה לפי כל דין, לצורך מילוי סמכויות העירייה ותפקידיה לפי כל דין, לאחר שהעירייה שוכנעה שההתקשרות נדרשת מטעמי חיסכון ויעילות והיא מיטיבה עם העירייה".

בהתאם להוראות סעיף 1 לחוק הפרשנות, תשמ"א-1981, הגדרת המונח "רשות מקומית" הינה "עיריה, מועצה מקומית, ועד מקומי או איגוד ערים."

בצו איגודי ערים (אשכול רשויות השרון), תשע"ח-2018 נקבע כי אשכול רשויות השרון מהווה "איגוד ערים", ועל כן עולה כי התקשרות של העיריה עם האשכול עונה על הקריטריונים הקבועים בתקנות המכרזים. יש לזכור כי הצטרפותה של עיריית הוד השרון לאשכול רשויות השרון טרם אושרה ע"י משרד הפנים ועל כן יש לנהוג במשנה זהירות.

מאחר ובמועד התכנסות וועדת השלושה משרד הפנים טרם אישר את צו האיגוד, אישרה וועדת השלושה את ההתקשרות לתקופה מוגבלת של 3 חודשים כמפורט להלן:

**החלטת הוועדה**

**לאור הצורך הדחוף מבחינה מקצועית ותקציבית ולאור העובדה שקבלת העירייה לאשכול הינה בשלביה האחרונים אנו מאשרים להתקשר עם האשכול ב"הסכם מנמ"ריה" בכפוף להלן:**

1. **יתווסף סעיף בהסכם ההתקשרות הקובע כי במידה ולא יתקבל אישור משר הפנים לקבלת העירייה לאשכול בתוך 6 חודשים, ההסכם יבוא לסיומו.**

2. **ההתקשרות לקבלת שירותי אבטחת המידע בסך של 12,500 ₪ (כולל מע"מ לחודש עבור 40% משרה) תוגבל ל-3 חודשים בשלב זה. עם זאת במידה ויתקבל אישור משרד הפנים לקבלת העירייה לאשכול, ניתן יהיה להמשיך בהתקשרות עד לתום התקופה הקבועה בהסכם מול האשכול.**

להבנת הביקורת ההתקשרות וקבלת השירות והתשלום נמשכו ונמשכים ברציפות עד ליולי - אוגוסט 2021 (כחודשיים ממועד מינוי ע"י המנכ"ל של ממונה בטיחות מידע) למרות שאישור משרד הפנים ניתן רק בינואר 2021. ראה נספח י"ב.

לתפיסת הביקורת אי קיום / הפרת החלטת וועדת השלושה (תוקף החלטת וועדת השלושה הסתיים ב-4/8/20) מהווה פגיעה בחוק (תקנות העיריות), פגיעה בכללי מינהל תקין וליקוי בהתנהלות להתקשרות חוזית עם ספק.

**<u>הביקורת ממליצה</u>** לבחון אירוע זה בפירוט ובהתאם לממצאים לפעול לפעילות מתקנת ולפעילות שתמנע הישנות אירוע כזה בעתיד.

# 7. וועדת היגוי לאבטחת מידע

במטרה לקדם את נושא אבטחת המידע הוקמו בארגונים רבים ועדות היגוי לנושא אבטחת המידע והגנת הפרטיות.

7.1. **הרכב מקובל של וועדת היגוי**

7.1.1. מנכ"ל העירייה ( ראה סעיף 8.3.3 להלן).

7.1.2. מנמ"רית העירייה.

7.1.3. מנהל אבטחת המידע באגף מערכות מידע.

7.1.4. גזבר העירייה.

7.1.5. היועץ המשפטי.

7.1.6. קצין הביטחון.

7.1.7. מנהל/ת משאבי אנוש.

7.1.8. מנהל אגף התפעול.

7.1.9. מנהלת החברה הכלכלית.

7.1.10. הממונה על חוזים והתקשרויות.

7.2. **תפקידים מקובלים של ועדת היגוי**

7.2.1. אישור ועדכון בכל הנוגע למדיניות אבטחת המידע ונהלים.

7.2.2. להנחות, לפקח ולסייע בכל הקשור לניהול תקין של אבטחת המידע בעירייה.

7.2.3. אישור תוכניות העבודה בתחום אבטחת מידע, הקצאת תקציבים ומעקב אחר יישום.

7.2.4. מיתווה עקרוני לתוכניות העבודה בתחום.

7.2.5. לדון באירועי אבטחת מידע חריגים.

7.2.6. להבטיח קיומם של מנגנוני פיקוח ובקרה נאותים.

7.2.7. לסייע להנהלת העירייה בקבלת החלטות בכל הקשור לתחום אבטחת המידע, מתוך ראיה אינטגרטיבית של התחום בעירייה.

7.2.8. קבלת דיווחים תקופתיים ממונה אבטחת מידע והנחיית ממונה אבטחת המידע.

7.2.9. להעלות יוזמות ו/או לדון ביוזמות לפרוייקטי פיתוח שכלול ושידרוג בנושא אבטחת מידע.

7.3. **סדרי עבודה מקובלים לוועדת ההיגוי**

7.3.1. הוועדה תתכנס בתדירות מספקת שתקבע, אך לא פחות מאחת לשנה.

7.3.2. הוועדה תדווח לראש העירייה ולמנכ"ל על פעילותה ועל מסקנותיה והמלצותיה בנושאים בהם הוסמכה לעסוק, הוועדה תערוך פרוטוקולים של ישיבותיה.

7.3.3. רצוי כי בדיון השנתי בו תאושר תכנית העבודה ותקציבים יהיה נוכח מנכ"ל העירייה וכן נוכחותו לפחות פעמיים בשנה.

7.4. **ממצאים:**

7.4.1. התייחסות מנהלת האגף למערכות מידע "נושא וועדת ההיגוי:

בעבר היו זימונים, אך עקב אירועי השנה האחרונה וחילופי מנהלים, הוועדה לא התכנסה בפועל באופן שוטף, אלא עפ"י צרכים נקודתיים שהועלו, כגון וועדות להעברות מידע בין גופים ציבוריים, הקמת מצלמות משטרה, שימוש במידע בזמן חירום, העברת מידע מגוף ציבורי בהקשר למיזם לביטחון תזונתי למשפחות מוחלשות, "

7.4.2. פגישת וועדה היגוי לאבטחת מידע

הביקורת מצאה, על בסיס צילום שנתקבל מהאגף (נספח י"ג), כי רק פעם אחת בשלוש השנים האחרונות (2019 עד 2021), בתאריך 30/12/2020 היה זימון למפגש צוות בכיר

(בחלקו), לכאורה כעין צוות היגוי לנושא אבטחת מידע. זומנו למפגש: המנכ"ל, הגזבר, המנמ"רית, מנהל אגף אבטחת מידע, סגן ראש העיר – מאיר חלוואני, היועמ"ש. כמו כן: מנהלת לשכת הגזבר, מזכירת הלשכה המשפטית, מזכירת תקשורת מנמ"רית, עוזר מנכ"ל.

<u>עפ"י הזימון אין לדעת</u>:

- האם אכן הזימון הינו לישיבה כוועדת היגוי לעניין אבטחת מידע?
- לאיזה חלון זמן בתאריך הזימון הייתה הישיבה מתוכננת?
- האם אכן הייתה בכלל ישיבה?
- אם אכן הייתה ישיבה, מי השתתף בה בפועל?
- אם אכן הייתה ישיבה, מה הנושאים שנדונו בה?

<u>יודגש כי לא נתקבל פרוטוקול לישיבה זו. (הביקורת ביקשה פרוטוקולים)</u>

7.4.3. פגישות שונות לעניין מידע, נתונים ואבטחת מידע

נתקבל מהמנמ"רית צילום של 17 זימונים לפגישות (חלקן בזום) לעניין מידע ותקשורת במהלך תקופה של כ- 15 חודשים (מפברואר 2020 עד מאי 2021). רוב הפגישות תוכננו לענייינים שוטפים ומיעוטם בעלי אופי עקרוני בין מערכתי. לצילום הזימונים ראה נספח י"ד.

לא הועברו לביקורת כל נתונים מתועדים המבהירים אם אכן התקיימו הפגישות, נושאי הדיון והמשתתפים בהם. לאמור: <u>לא נתקבלו כל פרוטוקולים או מסמכים מסכמים ביחס לפגישות.</u>

**7.5. תפיסת הביקורת ומסקנותיה**

7.5.1. תפיסת הביקורת

לתפיסת הביקורת תיפקוד סדיר, רציף ומקצועי המשולב במחויבות מעשית של וועדת היגוי לאבטחת מידע, הינו בעל חשיבות רבה ותרומה מהותית לניהול נושא אבטחת המידע והגנת הפרטיות בעירייה.

7.5.2. מסקנות הביקורת

מהחומרים שהתקבלו בביקורת מהאגף, הביקורת מגיעה למסקנות הבאות:

7.5.2.1. לא הוגדרה באופן פורמאלי ועדת היגוי לנושאי אבטחת מידע באמצעות כתב מינוי, או במסגרת נוהל ארגוני לרבות תפקידיה, סמכויותיה וחבריה.

7.5.2.2. לפחות בשנים האחרונות (2019 – 2021) אין התכנסות של צוות כוועדת היגוי (גם אם לא מונה פורמאלית) לעניינים שוועדת היגוי לאבטחת מידע צריכה לדון בהם, כמפורט בסעיף 7.2 לעיל.

7.5.2.3. אין תיעוד המאמת התכנסות של ממלאי תפקיד בכירים בעירייה (כאלו או אחרים), לעניינים הנוגעים במישרין או בעקיפין לאבטחת מידע.

7.5.2.4. לנוכח תפיסת הביקורת והמסקנות הנ"ל הביקורת מוצאת בנושא זה של וועדת היגוי פערים בהתנהלות הנושא, שאיננה הולמת את חשיבותו בעירייה.

7.5.3. המלצות הביקורת

- להגדיר פורמאלית ועדת היגוי לנושאי אבטחת מידע לרבות הרכבה, תפקידיה וסמכויותיה.
- לכנס ועדת היגוי בתדירות תקופתית כולל דיון עם מנכ"ל העירייה, לפחות אחת לחצי שנה.

### 7.6. תגובת האגף לטיוטת דוח הביקורת והתייחסות הביקורת

#### 7.6.1. תגובת האגף

**5. סעיף 7 ועדת היגוי לאבטחת מידע**

אין כל חובה חוקית למינוי ועדה זאת, יחד עם זאת האגף רואה חשיבות בסקירה שנתית של מצב קיים היבטי אבט"מ וסייבר ולכן יקיים פגישת סטטוס אחת לשנה בהשתתפות נציג הנהלה.

מטרת הפגישה: הצגת תכנון מול ביצוע וקבלת החלטות בהתאם לנדרש בכל הקשור בהיבטי אבטחת מידע והגנות סייבר.

#### 7.6.2. התייחסות הביקורת

הביקורת לא כתבה בטיוטת דוח הביקורת כי קיימת חובה חוקית למינוי וועדת היגוי.

לתפיסת הביקורת, הצעת הנהלת האגף לפגישת סטטוס אחת לשנה בהשתתפות נציג ההנהלה איננה נותנת מענה לרציונל בהקמה והפעלה סדורה של וועדת היגוי. הצעת הנהלת האגף איננה נותנת ביטוי מספק לרמת הסיכון ההולכת וגוברת בקצב גבוה בכל הנוגע לסיכוני אבטחת מידע ומתקפות סייבר.

הביקורת ממליצה לאמץ את המלצתה כמפורט לעיל בסעיף 7.5.3 .

# 8. מאגרי המידע

8.1. **כללי**

חוק הגנת הפרטיות התשמ"א 1981, מהווה את הבסיס החוקי לניהול מאגרי המידע. סעיף 8 לחוק קובע את החובה

8.2. **רשימת מאגרי המידע בעירייה**

8.2.1. מספר מאגרי מידע

לפי טבלת אקסל, שנקראת "רישום מאגרי מידע" שנתקבלה מהאגף, קיימים בעירייה ובשימוש העירייה 21 מאגרי מידע. (נספח ט"ו). להבנת הביקורת טבלה זו הינה מסמך מרכז של מאגרי מידע המנוהל באגף.

8.2.2. התייחסות הביקורת לטבלה המרכזת של מאגרי המידע בעירייה

8.2.2.1. פרטים בטבלה המרכזת

לתפיסת הביקורת, עצם ניהול מאגרי המידע של העירייה בטבלה מרכזת הינה התנהלות נכונה. טבלה זו הינה למעשה מיפוי והגדרת כל המאגרים, כפי שנדרש עפ"י חוק הגנת הפרטיות. יצוין כי כל רשומה בטבלה, שמבטאת מאגר מידע אחד, משתרעת על 66 עמודות ! עם פרטים רבים כפי שהחוק דורש לרבות:

-שם המאגר ומטרותיו.
-שמו ותפקידו של מנהל מאגר המידע, או המחזיק בו.
-מספר אנשים שפרטיהם כלולים במאגר.
-מספר משתמשים.
-האם יש גופים חיצוניים לעירייה המחזיקים במאגר ומיהם.

עם זאת הביקורת מצאה כי מתוך 66 עמודות שבטבלה, 26 עמודות הינן ללא תוכן כלל. (רשומות, לכאורה, רק לצאת ידי חובה). יש בכך לתפיסת הביקורת פגם.

8.2.2.2. תאריך

הטבלה איננה נושאת כל תאריך כך שלא ניתן להבין מתוכה למתי המידע שבה עדכני.
<u>הביקורת רואה בהיעדר תאריך על מסמך כזה (שאמור להיות מסמך מבוקר) ליקוי מהותי.</u>

8.2.2.3. מספר זיהוי לכל מאגר

למרבית המאגרים הרשומים בטבלה ניתן מספר מזהה בן 5 ספרות שמתחיל ב-8.
לתפיסת הביקורת מספר מזהה חד ערכי לכל מאגר ראוי לציון חיובי.
עם זאת, חלק מהמאגרים נרשמו, כפי שהחוק מחייב, בפנקס מאגרי המידע ברשות

להגנת הפרטיות – משרד המשפטים. ברישום זה ניתן לכל מאגר מידע מספר מאגר ברישומי הפנקס. מספר זה שונה מהמספר הרשום בגיליון ריכוז המאגרים באגף.
לתפיסת הביקורת יש בכך ליקוי והיה ראוי שתהה אחידות בזיהוי המאגר בשני הרישומים.

8.3. **רישום בפנקס מאגרי המידע ברשות להגנת הפרטיות - משרד המשפטים (להלן: "רישום")**

8.3.1. ממצאי ומסקנות הביקורת

8.3.1.1. במועד תחילת הביקורת אין רישום

נכון ל- 21 באפריל 2021 , תאריך התחלת הביקורת ( העברת שאלון לנתונים לביקורת מהמבקר אל מנהלת האגף), אין לביקורת כל תיעוד על מאגר כלשהו שהיה רשום בפנקס מאגרי המידע ומכאן שלמסקנת הביקורת, במועד זה, לא היה לכאורה רישום כזה. יש בהיעדר הרישום, לכאורה, ליקוי מהותי והפרת חוק.

8.3.1.2. מאגרים הדורשים רישום

לראיית הביקורת, עפ"י חוק הגנת הפרטיות, מתוך 21 מאגרי המידע הרשומים בטבלת ריכוז המאגרים, לפחות 19 מאגרים דורשים רישום. לפירוט התנאים לרישום עפ"י חוק הגנת הפרטיות ראה נספח ט"ז.

8.3.1.3. מאגרים רשומים בפועל ומועד הרישום

הביקורת מצאה בי בפועל נרשמו בפנקס המאגרים רק 8 מאגרים ( כ- 42%) מכלל המאגרים הדורשים רישום. לפרטי המאגרים הרשומים ראה נספח י"ז.
כל המאגרים הרשומים נרשמו בתאריך 12/5/2021. ל- 2 דוגמאות רישום ראה נספח י"ח.
הביקורת רואה ברישום חלקי זה ומאוחר (רק לאחר מועד תחילת הביקורת) של המאגרים, ליקוי מהותי והפרת חוק.

8.3.2. המלצות הביקורת בעניין רישום המאגרים

הביקורת ממליצה לפעול בהקדם להשלמת הרישום של כל מאגרי המידע הטעונים רישום עפ"י החוק.

8.4. **המלצות הביקורת לעניין מאגרי המידע**

הביקורת ממליצה לפעול בהקדם לתיקון כל הליקויים והפגמים שהביקורת מצביעה עליהם בפרק זה ( פרק 8.)

8.5. **ממצאי - דוח סטטוס אבטחת מידע מ-08/08/2020**

בדוח סטאטוס שנערך ע"י ר.א. - מנהל מידע אשכול רשויות השרון נכתב בנושא זה נאמר:

מאגרי מידע - ממידע הנמצא במשרד המשפטים ישנם 4 מאגרי מידע רשומים , ממיפוי מערכות הליבה בעירייה עולה באופן ברור, כי יש חוסר ברישום מאגרי מידע ובנוסף עולה כי המנמ"רית הקודמת בתפקיד, רשומה כמנהלת כלל המאגרים בעירייה , נעשה מיפוי ונדרש להחתים את מנהלי המאגרים החדשים על המאגרים הרשומים והמאגרים שעתידים להירשם.

התייחסות הביקורת: ממצאים אלו מצטרפים לממצאי הביקורת, מאששים את מסקנותיה לעיל (עם ההתאמות הנדרשות מהתאריכים של דוח הסטאטוס ודוח הביקורת) ותומכים בהמלצותיה.

8.6. **תגובת האגף לטיוטת דוח הביקורת והתייחסות הביקורת**

8.6.1. **תגובת האגף**

**6. סעיף 8 מאגרי מידע**

בעת כתיבת מענה זה, מבוצעת הערכת סיכונים על ידי חברה חיצונית בלתי תלויה. לאחר קבלת ממצאי העבודה (אשר כוללת בין היתר גם את נושא מאגרי המידע), יטופלו כלל הליקויים והחריגות מחוק הגנת הפרטיות ומהתקנות.

8.6.2. **התייחסות הביקורת**

לתפיסת הביקורת נדרש כי הצהרת הכוונות של הנהלת האגף לתיקון הליקויים והחריגות תלווה בלוח זמנים מחייב, שאותו לא פרס האגף בתגובתו לטיוטת דוח הביקורת.

# 9. סקר סיכונים

9.1. **כללי**

9.1.1. הבסיס הלוגי / רעיוני של סקר הסיכונים

במערכות אבטחת מידע מתקיימים, כמו בכל מערכת ניהולית, נקודות חולשה (ועוצמה) ואיומים המתורגמים לסיכונים.

הנהלת העירייה באמצעות הנהלת האגף צריכים לנקוט בפעילות אקטיבית לניהול סיכונים אלו, הכוללים ראשית זיהוי, שנית הערכת עוצמתם ושלישית פעילות להפחתת החשיפות אליהם.

אחת מפעולות המניעה החשובות בעניין זה, הינה סקר סיכונים בנושא אבטחת מידע. סקר הסיכונים אמור להשיג את היעדים הבאים:

זיהוי ואיתור הסיכונים והאיומים להם חשופה מערכת המידע / המחשב.

זיהוי מערכות המידע הרגישות בעירייה.

הצגת הסיכונים שנמצאו, לרבות סיכויי התממשותם והנזק הפוטנציאלי באם יתממשו.

הצגת פעילות נדרשת להפחתת החשיפות וההסתברות להתממשות ולהפחתת מידת הנזק אם יתממשו.

9.1.2. לשון החוק

בסעיף 5 בתקנות הגנת הפרטיות (אבטחת מידע) התשע"ז - 2017 נקבע:

"**(ג )** במאגר מידע שחלה עליו רמת האבטחה הגבוהה[1] 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.

**(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. "

9.2. **סקר סיכונים באגף**

9.2.1. <u>כללי</u>

בחודשים יולי-אוג' 2018 נערך סקר סיכוני אבטחת מידע על מרבית משאבי המידע והמחשוב בעירייה ע"י חברה חיצונית .Mad Sec Security ltd . ביצוע הסקר בהתאמה לדרישות החוק, הינה פעילות נכונה הראויה לציון חיובי.

9.2.2. <u>מסקנה מרכזית ועיקרית של הסקר</u>

לאחר שקילת פגיעויות האבטחה שנמצאו, אל מול ניתוח חשיבות המידע כפי שאופיין הן ברמת בדיקות החדירות והן בסקר הסיכונים המקיף, להערכתנו מערכות המידע "בעירייה" חשופות לאיומים <u>ברמת סיכון גבוהה</u>.

9.2.3. <u>איומים וסיכונים - ממצאים בסקר ושיטת הפירוט:</u>

כל ממצא זכה בסקר לפירוט מלא וכלל:

- רמת הסיכון
- תיאור האיום

---

[1] במאגרי המידע של העירייה הביקורת מזהה כי לפחות על חלק מהמאגרים חלה רמת אבטחה גבוהה. להגדרה עפ"י התקנה מתי חלה רמת אבטחה גבוהה ראה נספח י"ט.

- תיאור הממצא
- המלצות לתיקון / להפחתת הסיכון

9.2.4. <u>איומים וסיכונים - ממצאים בסקר לפי נושאים:</u>

מוצגים כאן רק סיכונים שבהם חומרת הנזק גבוהה או בינונית והסבירות להתרחשות הסיכון גבוהה ובינונית.

נמצאו ממצאים במערכות / נושאים הבאים:

(1) קומפלוט.
(2) הפרדת סביבות.
(3) מידע ארגוני על מחשבים נייחים ונישאים.
(4) ניהול Firewall.
(5) הרשאות עובדים.
(6) עדכוני אבטחה - שרתים ועמדות.
(7) הפרדת סמכויות - ניהול הרשאות ADMIN.
(8) הקשחת שרתים ועמדות קצה.
(9) חיבור VPN ללא הזדהות חזקה.
(10)מדיניות ניהול סיסמאות.

פירוט ניתן לראות (למורשים בלבד) במסמך סקר הסיכונים, שלא צורף מטעמי חיסיון מידע.

9.2.5. <u>ממצאים - בדיקות חדירות פנימיות</u>

מוצגים כאן רק ממצאי בדיקת חדירות שבהם חומרת הנזק קריטית וגבוהה או בינונית והסבירות להתרחשות הסיכון קריטית, גבוהה ובינונית.

נמצאו ממצאים במערכות / נושאים הבאים:

(1) שליטה מלאה על שרתי הארגון בעקבות מחסור בעדכוני אבטחה.
**(2)** שימוש במערכות הפעלה בלתי נתמכות.
(3) זיהוי מחשבי עובדים ברשת ה Wi-Fi -אורחים.
(4) חשיפת קבצים בשירות NFS.
**(5)** חשבון Administrator מקומי מכיל סיסמה חלשה.

**גם במקרה זה** פירוט ניתן לראות (למורשים בלבד) במסמך סקר הסיכונים, שלא צורף מטעמי חיסיון מידע.

9.3. **פעילות מתקנת**

9.3.1. <u>פעילות שבוצעה עפ"י נתונים מהאגף</u>

לשאלת הביקורת "אם נעשו פעולות להפחתת סיכונים ולפתרונות למניעת חדירה בעקבות הסקרים: נא להמציא תיעוד", נתקבל מענה האגף כדלקמן:

1. שודרגה מערכת FW.
2. שודרגה מערכת AV.
3. שודרגה מערכת PROXY.
4. החלה סגמנטציה.
5. שודרגה מערכת AD.
6. הופעלה מערכת AUDIT.
7. שודרגה מערכת הפעלה לש עמדות.

9.3.2. <u>התייחסות הביקורת לנתוני האגף על שדרוגים</u>

למסקנת הביקורת מענה האגף איננו נותן מענה לסיכונים והאיומים – בעיקר לאלו שחומרת הנזק בהם קריטית, גבוהה או בינונית ושהסבירות להתממשות גם כך: קריטית, גבוהה או בינונית.

כפי שפורט בסעיפים 9.2.4 ו-9.2.5 לעיל בסקר הסיכונים נמצאו 10 גורמים/ אמצעי מיחשוב / תהליכים ברמת סיכון גבוהה או בינונית. (חומרה או הסתברות מימוש). בנוסף בבדיקות חדירות פנימיות נמצאו 5 גורמים ברמת סיכון קריטית או גבוהה או בינונית. סה"כ - **15** ממצאים שונים.

מול זאת מציג האגף פעילות שדרוג או שינוי ב- **7** גורמי מחשוב.

מתוך 7 הגורמים ששודרגו או שונו הביקורת מזהה בוודאות מענה לממצאי סקר הסיכונים רק בגורם אחד - מס. 4 ברשימה שהתקבלה מהאגף: " החלה סגמנטציה". לא ברור מתוך הגדרה זו מתי החלה סגמנטציה, מה שיעור השגת הסגמנטציה עד כה, מול הצורך ומתי עתידה פעילות זו לתת מענה לפער המהותי ולסיכון הגבוה הנגזר ממנו, כפי שנמצא בסקר הסיכונים. לתפיסת הביקורת המהלך שמוגדר "החלה סגמנטציה" הוא בכיוון הנכון, אבל לנוכח הפירוט הנ"ל, אין הביקורת יכולה להתייחס אליו כבעל תרומה ממשית (עד כה ) להפחתת סיכוני היעדר הסגמנטציה.

לגבי יתר 6 השדרוגים: לדעת הביקורת, כנראה שיש בהם תרומה להפחתת הסיכונים המוצגים בסקר הסיכונים, אבל לא ברור לאיזה ובאיזה מידה. לתפיסת הביקורת, היה ראוי שאל מול כל סיכון מזוהה בסקר, יפורט השדרוג שבא לתת לו מענה וכיצד וכמה ומתי.

כך שלמסקנת הביקורת ביחס ל- 7 השדרוגים המוצגים הנ"ל, לא ניתן לדעת אם יש בהם מענה כלשהו לסיכונים המוצגים בסקר ואם כן באיזה מידה, באיזה קצב וכיו"ב.

<u>לסיכום</u>: הביקורת איננה רואה מתוך התיעוד שנתקבל בביקורת פעילות שלמה להפחתה משמעותית בסיכונים העולים מתוך הסקר (לפחות בקריטיים ובגבוהים שבהם). קיימת לכאורה פעילות חלקית וגם היא ללא אפשרות לייחס קשר מובהק בינה לבין השפעה ספציפית על סיכון כזה או אחר. הביקורת גם איננה רואה ניהול שיטתי של הסיכונים בנושא אבטחת מידע. לא ידוע על כל סקר סיכונים נוסף, לזה שבוצע בשנת 2018.
הביקורת ממליצה על השלמת הפערים עליהם מצביעה הביקורת.

9.4. **ריכוז נושאים לטיפול אבטחת מידע**

בביקורת נתקבל מהאגף קובץ אקסל בשם "ריכוז נושאים לטיפול אבטחת מידע" ובו 3 גיליונות:

(1) ממצאי סקר סיכונים.
(2) תחקיר אגף הסייבר.
(3) מטלות כללי.

הביקורת תתייחס רק אל גיליון ממצאי סקר סיכונים.

9.4.1. <u>פעילות להפחתת סיכונים אל מול ממצאי הסקר</u>

הביקורת מצאה בגיליון פריסה שיטתית ומפורטת של פעילות מתקנת נדרשת להפחתת סיכונים, של כל ממצא משמעותי, שנמצא בסקר (כאמור בסעיף 9.3.2 לעיל, 15 ממצאים כאלו). כמו כן נרשמה לכל פעולה מי אחראי ליישמה ובחלק מהן מה הסטאטוס של הטיפול. כל אלו ראויים להערכה חיובית.

עם כל זאת, מתוך הגיליון ניתן ללמוד כי :

(1) מתוך 24 פעולות מתוכננות להפחתת הסיכונים, רק ב-15 מהם נרשם סטאטוס. לגבי 9 מהם (כ- 38%) אין כל התייחסות.
(2) מתוך 15 שורות סטאטוס לפעולות הפחתת סיכונים, למיטב הבנת הביקורת, רק ב-2 מהן (8%) ניתן לראות עפ"י הסטאטוס הרשום ביצוע בפועל: (1) שורה 23 - חסימת USB ; (2) שורה 24 - החלפת סיסמאות.

בכל יתר השורות הסטאטוס מבטא המלצה ליישום הפעולה, או פרוט טכני לתיאור הפעולה.

(3) אין בכל הגיליון ובכל הקובץ על 3 הגיליונות שבו, תאריך אחד לרפואה. לא מהו תאריך הקובץ, ולא תאריכי סטאטוס.[2] לפירוט גיליון האקסל האמור ראה נספח כ'.

9.5. **גיליון אקסל " אירועי אבטחת מידע"**

בנתוני האגף לביקורת נתקבל קובץ אקסל בשם " אירועי אבטחת מידע" ובו שני גיליונות:

גיליון מ- 06.2021 ובו מצוין אירוע אחד מיוני 2021 של דליפת מידע. (התייחסות הביקורת לנתון זה מוצגת בפרק 13 להלן " אירועי אבטחת מידע").

גיליון מ- מאי 2021 ובו תיאור של 7 סיכונים משמעותיים של אבטחת מידע, שהאגף זיהה שיכולים להביא לדליפת מידע ו/או לפריצה למאגרי המידע של העירייה. (ראה נספח כ"א)

בגיליון זה קיים תיאור של סוג הפגיעות מכל סיכון שזוהה והמלצה למניעתו ו/או להפחתתו. יודגש כי רק לגבי סיכון אחד (חיבור בו זמני ל-2 רשתות) מצוין בגיליון כי הנושא טופל.

מכאן הביקורת מגיעה למסקנה, כי כל יתר 6 הסיכונים לא טופלו וההמלצות לא יושמו. הביקורת רואה בזיהוי הסיכונים מהלך הראוי לציון חיובי ויחד עם זאת אי יישום, , של ההמלצות לטיפול, מהווה ליקוי מהותי.

9.6. **סיכום המענה להפחתת סיכוני אבטחת מידע אל מול סקר הסיכונים**

מתוך המוצג בסעיפים הקודמים של פרק 9. עולה כי מענה האגף להפחתת סיכונים, כצורך העולה מתוך סקר הסיכונים, הינו חלקי בלבד ואיננו מספק.

רוח החוק והתקנות והמציאות רוויית הסיכונים, כולל התממשות אירוע פריצה חמור בשנת 2020 מדגישים את החשיבות הרבה בהפחתת הסיכונים והאיומים כמוצג בסקר הסיכונים. לפיכך, מענה האגף החלקי מהווה לתפיסת הביקורת, פגם וליקוי ניהולי.

---

[2] הביקורת רואה בהיעדר תאריכים במסמך (ולא רק במסמך הזה של האגף) ליקוי חמור ופגם מהותי בתרבות הניהול ובתרבות הארגונית באגף.

הביקורת ממליצה להציב את יישום הפתרונות אל מול הפערים העולים מתוך הסקר במידרג עדיפות גבוה בהתאם ולפעול בנחישות למימוש. נדרש להכין תוכנית פעולה הולמת, לרבות לוח זמנים, אחריות ותיקצוב בהתאם.

9.7. **תדירות עריכת סקר סיכונים**

עפ"י תקנות הגנת הפרטיות (אבטחת מידע) התשע"ז – 2017, תקנה 5. סעיף (ג) " סקר סיכונים כאמור, יערך אחת לשמונה עשר חודשים לפחות.

סקר הסיכונים נערך בעירייה ביולי 2018. עפ"י התקנות נדרש כי ייערך סקר סיכונים נוסף ב- דצמבר 2019. לא התקבל בביקורת כל תיעוד בנוגע לסקר כזה ולפיכך הביקורת מסיקה כי לא נערך.

הביקורת מוצאת אי קיום סקר סיכונים כנדרש במשך של כ- 20 חודשים ( אוגוסט 21 - מועד כתיבת טיוטת דוח הביקורת ) כליקוי מהותי והפרת חוק.

הביקורת ממליצה לפעול בהקדם לתיקון הליקוי גם בגלל החוק וגם בגלל הסיכונים והאיומים הריאליים הקיימים הלכה למעשה.

9.8. **תגובת האגף לטיוטת דוח הביקורת והתייחסות הביקורת**

9.8.1. **תגובת האגף**

**7. סעיף 9 סקר סיכונים**

העירייה התקשרה, כאמור, בעת האחרונה עם חברה חיצונית המבצעת פעילויות הערכת סיכונים כולל מבדקי חדירה וסקר סיכונים אשר מבוצעים בעת כתיבת שורות אלה. כמו"כ שכרה העירייה את שירותיה של חברת חלוקי נחל לייעוץ אבטחת מידע והגנות סייבר.

בסיום הפעילויות הללו, תבוצע הערכת הסיכון ותכתב תכנית מותאמת להפחתת הסיכון עד לאישור סיכון קביל או עד לקבלת מיטיגציה מלאה.

9.8.2. **התייחסות הביקורת**

גם בסעיף זה, לתפיסת הביקורת נדרש כי הצהרת הכוונות של הנהלת האגף לפעילות של הפחתת סיכונים תלווה בלוח זמנים מחייב, שאותו לא פרס האגף בתגובתו לטיוטת דוח הביקורת.

# 10.מאגרי המידע : אבטחה פיזית וסביבתית

10.1. **בקשות הביקורת מהאגף לנתוני האבטחה הפיזית והסביבתית**

הביקורת ביקשה מהאגף פרטים ביחס לסידורי האבטחה הפיזית והסביבתית למאגרי המידע כדלקמן:

1.באיזורי / מקומות עבודה: נא להמציא פירוט ותיעוד על סידורים ופתרונות לאבטחה פיזית וסביבתית, כולל: (א) מסמכים על שולחנות, (ב) קבלת קהל, (ג) מצלמות במעגל סגור, (ד) מערכות אזעקה וחיישנים למקומות רגישים, (ה) מערכות כיבוי אש למקומות אחסון מסמכים חשובים / רגישים.

2.אם מתבצעות בקרות מתועדות נא להמציא תיעוד.

3.באזור המחשוב וחדר / י השרתים: נא להמציא פרטים ותיעוד על סידורים לאמצעי זיהוי.

4.חדר/י חדר שרתים: (א) מיקום, (ב) זיהוי כניסה, (ג) הגנה בפני שריפות, (ד) הגנה בפני הצפות, (ה) תנאי סביבה ( בקרת טמפרטורה), (ו) הגנה להפסקת חשמל (אל פסק USP ו/או גנרטור).

10.2. **תשובת האגף והתייחסות הביקורת**

10.2.1. <u>נהלים והדרכה</u>

10.2.1.1. תשובת האגף

קיימים נהלים העוסקים בגישה פיסית למידע,
עובד, בקבלתו לעבודה נדרש לחתום על טופס שמירת סודיות ונהלי אבטחת מידע,
חלקם אף מקבלים הדרכה בכניסתם לתפקיד.
כמו"כ ישנו נוהל לאבטחה פיסית.
יש צורך בשיפור תחום זה ע"י העלאת מודעות, לכלול נושא זה בהדרכות המתוכננות,
תזכורות במייל מידי פעם וכיוצ"ב.

10.2.1.2.התייחסות הביקורת

**נהלים**

הצהרת האגף שיש נהלים בנושא מספקת מענה חלקי ומועט לעניין הנהלים. כאמור בסעיף 3. לעיל, ממצאי הביקורת הינם כי נושא הנהלים לקוי במידה מהותית ויש בניהולם פגמים משמעותיים לרבות היעדר מספרי זיהוי, כפילויות, סדר עריכה, תיארוך ועוד. לפיכך אין זה מעשי כי הביקורת תנסה לגשש את דרכה במבוכי "יער" הנהלים שהאגף שלח אליה ולדלות מתוכם את הנהלים שאליהם מכוון האגף.

**היה מוטב שהאגף היה מפרט מהם הנהלים ( מספרי זיהוי, שם וכיוצ"ב) וכמו כן מצרף את הנהלים.**

**הדרכה**

לדברי האגף, רק חלק מהעובדים מקבל הדרכה בכניסתם לתפקיד. לא מצוין איזה חלק האם 99% מהם או רק 1% מהם. לתפיסת הביקורת היה מאד ראוי כי נתון האגף יהיה יותר ספציפי וממוקד. (לביקורת יש כישורים רבים אך הניחוש איננו נמנה עליהם).

מהותית, לדעת הביקורת, אי הדרכה של חלק מהעובדים בכניסתם לתפקיד בנושא כל כך חשוב ורגיש, מהווה ליקוי מהותי וחמור.
הביקורת ממליצה להשלים הדרכות ולהתקין אמצעי בקרה הולמים שיבטיחו הדרכה בנושא, לכל עובד רלוונטי שנוגע לעניין.

כמו כן, נדרש לנהל באופן שוטף תוכנית הדרכות וריענונים מחייבת, לרבות אמצעי בקרה הולמים להבטחת מימושם.

10.2.2. <u>חדרי שרתים</u>

10.2.2.1. תשובת האגף

ישנם 3 חדרי שרתים, כולם נעולים בדלתות פלדה ומנעולי רב-בריח.
בכניסה לחדר נדרש להקליד את הקוד האישי לנטרול האזעקה,, אחרת מערכת אזעקה העירונית מופעלת.
מערכות בחדרי שרתים: מער' כיבוי אש יבשה, חיישן הצפה, חיישן טמפרטורה, גיבוי חשמל (UPS/ גנרטור נייד).
בחדר אחד מתוך ה- 3 (גזברות) אין מערכת כיבוי אש יבשה ואין חיבור לגנרטור. נדרש להשלים.

10.2.2.2. התייחסות הביקורת

תשובת האגף מהווה מענה מניח את הדעת לאבטחה פיזית וסביבתית לחדרי השרתים.
עם זאת היעדר מערכת כיבוי אש יבשה באחד החדרים והיעדר חיבור לגנרטור מהווה כמובן ליקוי מהותי ( ואפילו חמור על רקע המודעות שיש באגף לעניין).

לתפיסת הביקורת היעדרם של הנ"ל יוצר סיכון בלתי קביל שנדרש לפעול ללא דיחוי ולטפל בו. הביקורת ממליצה לממש תפיסתה זו בהקדם רב.

10.2.3. <u>סעיפים 1. ו-2. לבקשת הנתונים של הביקורת (סעיף 10.1 לעיל)</u>

לא נתקבלה כל התייחסות מהאגף לסעיפי אלו. על רקע זה הביקורת מגיעה למסקנה כי הנושאים האלו, , אינם מקבלים כל מענה באגף. יש בכך למסקנת הביקורת, ליקוי מהותי.

הביקורת ממליצה לתקנו (בכפוף לממצאי בדיקה מוקדמת ומפורטת ומעמיקה למצב לאשורו של הנושאים האלו).

# 11.אבטחת מידע בניהול כוח אדם והרשאות גישה

11.1. **בקשות הביקורת מהאגף לנתונים שבנושא הרשאות**

הביקורת ביקשה מהאגף פרטים ביחס לאבטחת מידע בניהול כוח אדם והרשאות גישה כר"מ:

(1)ניהול הרשאות גישה : רשימת הרשאות לפי תפקידים, זיהוי ואימות .

(2)ניתוק אוטומטי - פרק זמן לאי פעילות.

(3)טיפול בתקלות.

(4)ביטול הרשאות למסיימי תפקיד.

(5)בקרה ותיעוד גישה ( האם קיים מנגנון אוטומטי ?).

(6)הדרכות בנושא גישה והרשאות.

11.2. **התייחסות הביקורת**

לסעיפים (1) , (2), ו- (4) נתקבל מהאגף מענה מניח את הדעת.

לסעיפים (3), (5), ו-(6) לא נתקבלה מהאגף התייחסות. לפיכך מסקנה הביקורת הינה כי, , נושאים אלו אינם מטופלים ואינם זוכים לענה הולם. יש בכך ליקוי מהות.

הביקורת ממליצה לאגף לקיים בדיקה מעמיקה ומפורטת אחר המצב לאשורו בנושאים חסרי המענה ועפ"י הממצאים לפעול לתיקון הפערים והליקויים.

11.3.**תגובת האגף לטיוטת דוח הביקורת והתייחסות הביקורת**

11.3.1. **תגובת האגף**

**8. סעיף 11 – אבטחת מידע בניהול כוח אדם והרשאות גישה**

תכתב תכנית עבודה סדורה לווידוא כי נושאים 3,5,6 מטופלים, מבוקרים ומתועדים בהתאם.

11.3.2.**התייחסות הביקורת**

גם בסעיף זה, נדרש, לתפיסת הביקורת, כי הצהרת הכוונות של הנהלת האגף לפעילות מתקנת תלווה בלוח זמנים מחייב, שאותו לא פרס האגף בתגובתו לטיוטת דוח הביקורת.

# 12.אבטחת מידע - הדרכות

12.1.**בקשות הביקורת מהאגף לנתוני בנושא הדרכות**

הביקורת ביקשה מהאגף פרטים ביחס להדרכות אבטחת מידע כר"מ:

"(1) ככל שיש תוכניות הדרכה נא להמציא תיעוד על התוכניות ועל ביצוע לשנים 2019 עד 2021.

(2) אם גם נעשית בדיקת אפקטיביות נא לפרט ולהמציא תיעוד."

12.2.**התייחסות הביקורת**

מענה האגף לסעיף (1) לבקשת הביקורת מניח את הדעת:

"בשנות 2018-2020 עבדה מערכת CybeReady.

המערכת מדמה פישינג . בשנת 2020 נרכש מודול CAB - הינה תוספת הדרכה.

במהלך שנות 2018- 2019 בוצעו הדרכות פרונטליות:

אגף גזברות

ספרניות ביה"ס

מח' שפ"ח"

עם זאת, לדעת הביקורת:

ההדרכות ב- 2018 - 2019 מכסות אמנם יחידות ארגוניות חשובות, אבל אינן מכסות את כל היחידות בעירייה. שהיה ראוי להדריכם בנושאי אבטחת מידע.

היעדר הדרכות פרונטליות בשנים 2020 -2021 (גם אם היו אלו שנות קורונה ) מהווה לדעת הביקורת ליקוי מהותי. הביקורת רואה בכך ליקוי גם אם הועמדה לרשות משתמשי יחידות העירייה, מערכת CybeReady ( להדרכת מודעות לאבטחת מידע והתנהגות עובדים באוריינטציה של אבטחת מידע).

לסעיף (2): כמובן שהדרכה ללא בדיקת אפקטיביות הינה בעלת תועלת פחותה (אם בכלל). לא נתקבלה מהאגף כל התייחסות לנושא זה. מכאן הביקורת מסיקה כי, לא בוצעה כל בדיקת אפקטיביות שהימנעות ממנה מהווה ליקוי מהותי.

**הביקורת ממליצה** לקיים בדיקה מפורטת ומעמיקה לפערים לכאורה שמוצגים כאן ועפ"י הממצאים לבצע תיקון לליקויים ולפערים.

12.3.**תגובת האגף לטיוטת דוח הביקורת והתייחסות הביקורת**

12.3.1. **תגובת האגף**

**9. סעיף 12 – הדרכות אבטחת מידע**

בעת האחרונה מעודכנת לומדה אשר תופץ לכלל עובדי העירייה בנושאי אבטחת מידע. כמו"כ, תכתב תכנית הדרכות סדורה.

12.3.2. **התייחסות הביקורת**

גם בסעיף זה, לתפיסת הביקורת, נדרש כי הצהרת הכוונות של הנהלת האגף לפעילות של הפחתת סיכונים תלווה בלוח זמנים מחייב, שאותו לא פרס האגף בתגובתו לטיוטת דוח הביקורת. כמו כן בתגובת האגף אין כל התייחסות לעניין בקרת אפקטיביות ההדרכות שהיא, לתפיסת הביקורת, בחשיבות גבוהה לפחות כמו ההדרכות עצמן.

# 13.אירועי אבטחת מידע

13.1.**בקשות הביקורת מהאגף לנתוני בנושא אירועי אבטחת מידע**

הביקורת ביקשה מהאגף פרטים ביחס לאירועי אבטחת מידע בשנים 2019 עד 2021

13.2.**התייחסות הביקורת**

מענה האגף לבקשת הביקורת:

| תאריך | תאור | סוג פגיה | המלצות |
|---|---|---|---|
| | | | |
| 08.06.2021 | דליפת מידע על שיבוץ ילד בגן | דליפת מידע | |

במענה האגף אין כל נתונים לגבי המשמעות של דליפה המידע המתואר ולגבי הסיבות והגורמים שבגינם אירעה דליפת מידע זו. אין גם כל נתונים מה נדרש כפעילות מתקנת וכפעילות מונעת לעתיד. ראה את תגובת האגף לטיוטת דוח הביקורת להלן בסעיף 13.3.1.

<u>אירוע פריצה במרץ 2020</u>

למיטב ידיעת הביקורת התרחשה במרץ 2020 פריצת אבטחת מידע חמורה למערכות המידע של העירייה, באמצעות תוכנת רוגלה ודליפת מידע ביחס לתושבים ולעובדים. עפ"י פירסומים באינטרנט האירוע גם נבדק ע"י הרשות להגנת הפרטיות במשרד המשפטים והעירייה נקנסה בקנס של 10,000 ₪.

באופן תמוה (בלשון המעטה), אירוע זה לא מוזכר ולא גם במילה אחת, במענה האגף לבקשת נתונים של הביקורת להכנת טיוטת דוח הביקורת.

האירועים הנ"ל ממחישים את המשמעות המעשית של פערים בפעילות האגף למניעה והפחתת סיכונים - אל מול ממצאי סקר הסיכונים מ- 2018 ואל מול סיכונים שהאגף זיהה בהמשך לסקר הסיכונים, כפי שפורט בפרק 9. לעיל ("סקר סיכונים").

הביקורת רואה באי מתן מענה שלם ומלא לסיכונים שזוהו בפריצות ובדליפות המידע או בסקר הסיכונים או בזיהוי סיכונים ע"י האגף שלא במסגרת סקר הסיכונים, ליקוי מהותי ופגם מהותי בניהול נושא אבטחת המידע וממליצה לפעול בהקדם רב לתיקון הדברים. ראה להלן את תגובת האגף לטיוטת דוח הביקורת:

### 13.3.**תגובת האגף לטיוטת דוח הביקורת והתייחסות הביקורת**

13.3.1. **תגובת האגף**

**10.סעיף 13 – אירועי אבטחת מידע**

כלל אירועי אבטחת המידע טופלו ותוחקרו, קיים תחקיר אירוע מסודר בנוגע לפריצה ממרץ 2020. נהלי אבטחת המידע, לרבות נוהל טיפול באירוע מטוייבים בעת האחרונה, וכחלק מתהליך זה מוסדר גם נושא התחקירים.

13.3.2.**התייחסות הביקורת**

האגף לא העביר לביקורת, חרף בקשתה לחומרים בשלב הכנת טיוטת דוח הביקורת, חומרים על הטיפול והתחקור של האירועים.
גם בתגובת האגף לטיוטת דוח הביקורת האגף מסתפק בהצהרות ללא תיעוד נילווה וללא לוח זמנים לפעילויות טיוב הנהלים והסדרת התחקירים, כמוצהר.

# 14.אבטחת מידע - התקנים ניידים

14.1.**בקשות הביקורת מהאגף לנתוני אבטחת מידע בהתקנים ניידים**

הביקורת ביקשה מהאגף פרטים ביחס לאבטחת מידע, בהתקנים ניידים כר"מ:

"לקבל פירוט ותיעוד על דרכי היערכות להגבלה או מניעת אפשרות חיבור להתקנים ניידים. לקבל התייחסות לעניין הגנה על טלפונים ניידים, ו/ או טאבלטים המשמשים את עובדי העירייה בעבודתם.

14.2.**התייחסות הביקורת**

כמענה לבקשתה הועבר לביקורת אך ורק נוהל "אבטחת מידע בשימוש במכשירים ניידים". נספח כ"ב.

לתפיסת הביקורת תוכנו של נוהל זה והדרישה לחתימה על תוכנו מכל משתמש במכשיר נייד שמחובר לדוא"ל "הארגוני – "Exchange" מהווים גורמים לציון חיובי. עם זאת היה ראוי כי יועברו לביקורת מספר (מדגם קטן) של טפסי נוהל כזה, עם כל הפרטים המלאים, כולל תאריך וחתימת ממלא התפקיד החותם.

יודגש כי הנוהל שהועבר לביקורת איננו נושא כל לוגו או כל זכר וכל ציון שהמדובר בנוהל של עיריית הוד השרון, או של האגף למערכות מידע, עובדה תמוהה לכשעצמה.

כמובן שרק קיומו של נוהל איננו מבטיח היערכות אפקטיבית להגנה מסיכוני השימוש בהתקנים ניידים. נדרשים אמצעי מניעה ובקרה נוספים לכך. נתונים על אמצעים כאלו לא נתקבלו מהאגף בשלב הכנת טיוטת דוח הביקורת. ראה להלן את תגובת האגף לטיוטת דוח הביקורת ואת התייחסות הביקורת לתגובה זו.

14.3.**תגובת האגף לטיוטת דוח הביקורת והתייחסות הביקורת**

14.3.1. **תגובת האגף**

**11.סעיף 14 – התקנים נתיקים**

הנושא טופל על ידי אנשי אגף מערכות המידע במרץ 2020.

14.3.2.**התייחסות הביקורת**

תגובת האגף מסתפקת בהצהרה כללית ללא כל תיעוד כסימוכין.

# 15.הרשת הפנימית בעירייה - הגנה על גישה למאגרי מידע

לבקשת הביקורת לנתוני ההגנה הנ"ל, נתקבל מענה האגף כמפורט בנספח כ"ג.

**למסקנת הביקורת** - מענה האגף לנושא מניח את הדעת.

# 16.אבטחת תקשורת-חיבורים לרשת האינטרנט (או רשת ציבורית אחרת)

לבקשת הביקורת לנתוני ההגנה הנ"ל, נתקבל מענה האגף כמפורט בנספח כ"ד.

**למסקנת הביקורת** - מענה האגף לנושא מניח את הדעת.

# 17. אבטחת מידע בהתקשרות עם ספקי שירותי מערכות מידע

האגף העביר לביקורת נתונים ביחס להתקשרויות עם ספקי שירותי מידע הכוללים הסכמים ומסמכים הנוגעים לאבטחת מידע. הספקים שלהם התקבלו הסכמים או מסמכים הנוגעים להסכמים הינם:

(1)מלם שכר ; (2) סנסורי פתרונות תוכנה ; (3) מטרופולינט (4) קומפלוט ; (5) מילאון ; (6) מטריקס אי. טי. אינטגרציה ; (7) מגדלור מערכות זמן אמת.

## 17.1. מסמכי ההסכמים

מסמכי ההסכמים כוללים סעיפים ונספחים הכוללים את דרישות האגף לאבטחת המידע במהלך יישום ההסכם ע"י הספק. למסקנת הביקורת סעיפים ונספחים אלו מניחים את הדעת מבחינת דרישת האגף, זולת ההסכמים עם שתי החברות: האחרונות ברשימה:

17.1.1. **<u>חברת מטריקס</u>**

בהסכם עם חברת מטריקס אין כל התייחסות לחובותיה של חברת הספק בנושא אבטחת מידע, אין כל דרישות של האגף לכך ואין כל נספחים או טפסי הצהרה והתחייבות. לעמוד הראשון של ההסכם ראה נספח כ"ה.

17.1.2. **<u>מגדלור מערכות זמן אמת</u>**

בהסכם עם "מגדלור מערכות זמן אמת בע"מ" להספקה ותחזוקת שעוני נוכחות ואיסוף נתוני נוכחות של עובדי העירייה" קיים בהסכם סעיף מינורי בלבד, לנושא אבטחת מידע:

**שמירת סודיות ואבטחת מידע**

הקבלן מתחייב לשמור בסודיות כל מידע הנוגע לעירייה ולעבודיה שיגיע אליו, אגב, בקשר או במהלך ביצוע הוראות הסכם זה, ולאחסנם במקום ובאופן המתאימים ביותר, לשם שמירת סודיותם כאמור ולא למוסרם בין במישרין ובין בעקיפין לכל אדם ושאו גוף אחר וחכל בהתאם להוראת נספח אבטחת המידע המצורף להסכם זה כחלק בלתי נפרד ממנו.

כפי שניתן לראות לעיל, קיימת גם הפנייה בהסכם לנספח "אבטחת מידע". ההסכם שנתקבל בביקורת מהאגף, איננו כולל נספח כזה ולפיכך הביקורת מסיקה כי, לכאורה, נספח זה הוחמץ ולא נחתם ע"י הספק. הביקורת רואה בכך ליקוי מהותי ו**ממליצה** לבדוק לאשורו את הנושא ועפ"י ממצאי הבדיקה לפעול לתיקון הליקוי ולהפעלת אמצעי בקרה הולמים, למניעת הישנות החמצה כזו בעתיד.

## 17.2. טפסי הצהרה והתחייבות לאבטחת מידע

נשלחו אל החברות טפסי הצהרה והתחייבות, לעמידה בחוקי ותקנות אבטחת המידע. עצם העברת טפסים אלו ראויה לציון חיובי.

עם זאת, לביקורת לא הועברו טפסים החתומים ע"י החברות / הספקים. ולפיכך, הביקורת מסיקה כי ,לכאורה, באגף הסתפקו במשלוח הטפסים, בבחינת "יצא ידי חובה" אך לא "דאגו" גם לקבל אותם חתומים. יש בכך כמובן ליקוי שבעקבות בדיקה מעמיקה ובהתאם לממצאיה ראוי לתקנו ולהבטיח אי הישנותו בעתיד. לפירוט ראה נספח כ"ו

## 17.3. בקרות ואכיפה

על אף בקשתה, לא הומצא לביקורת כל תיעוד על ביצוע בקרה או פעילות אכיפה כלשהי בנושא אבטחת מידע כפי שהיה מצופה שיעשה – וכפי שהחוק והתקנות מחייבים.

**למסקנת הביקורת** יש בהימנעות מבקרת יישום הדרישות בהסכמים ובמסמכי ההצהרה וההתחייבות, ליקוי מהותי וחמור.

## 17.4. סקר סיכונים לספקים

אין באף אחד מההסכמים וממסמכי ההתחייבות וההצהרה דרישה של האגף מהספק, לביצוע סקרי סיכוני אבטחת מידע וסייבר.

**למסקנת הביקורת** יש בהיעדר דרישה זו, ליקוי מהותי וחמור.

**הביקורת ממליצה** לפעול בהקדם לתיקון ליקוי זה.

## 17.5. עמידה בתקן אבטחת מידע

אין באף הסכם עם הספקים דרישה להסמכה ממכון רישמי ( כמו מכון התקנים הישראלי) לעמידה בתקן אבטחת מידע (ISO 27001).

לתפיסת הביקורת דרישה כזו יכולה להבטיח מצד אחד לפחות מינימום יישום של דרישות הניהול לאבטחת מידע ומצד שני להקל על האגף באכיפה ובבקרה של קיום דרישות אלו.

נוכח זאת הביקורת רואה היעדר דרישה כזו, כפגם ופער בלתי רצוי בהתקשרויות עם ספק שרותי המידע לאגף.

הביקורת ממליצה לעתיד לשקול להוסיף דרישה כזו בהתאם לרוח הדברים הנ"ל.

## 17.6. לסיכום לעניין נושא אבטחת מידע בהתקשרויות עם ספקי האגף:

- הביקורת מוצאת בחלק מההתקשרויות סעיפים, נספחים ומסמכי התחייבות למלא אחר דרישות אבטחת מידע.
- אין כל תיעוד על אכיפת הדרישות הנ"ל בשיטות ובכלים שונים. לפיכך הביקורת מסיקה כי לכאורה, לא מתקיים מאומה מאכיפה זאת.
- הביקורת ממליצה לערוך בדיקה מעמיקה לסוגיה זו ובהתאם לממצאים, לתקן את הפגמים והליקויים.

### 17.7. תגובת האגף לטיוטת דוח הביקורת והתייחסות הביקורת

#### 17.7.1. תגובת האגף

**12. סעיף 17 - אבטחת מידע בהתקשרויות עם ספקים וגו"ח**

אגף מערכות מידע מקפיד לשלב נספחי אבט"מ בכל הליך התקשרותי הנוגע למערכת מידע.

ההתקשרויות אשר מוזכרות במסמך הביקורת הינן התקשרויות ישנות, בעבורן האגף יעביר נספחי אבט"מ ייעודים לחתימת הספקים.

בקרות ואכיפה – הסעיף איננו ברור.

כמו כן האגף יבחן התקשרות עם מערכת לביצוע סקרי ספקים.

נושא העמידה בתקן ISO27001:2013 יישקל באגף

#### 17.7.2. התייחסות הביקורת

לגבי תת הסעיף : "בקרות ואכיפה" שאיננו ברור להנהלת האגף:
כוונת הביקורת ב-"בקרות": בדיקה ובקרה ע"י האגף של מידת העמידה ומילוי הדרישות ע"י הספק אל מול המתחייב על פי ההסכם בנושא אבטחת מידע.

כוונת הביקורת ב- "אכיפה": פעילות ו/או סנקציות (עפ"י המתאפשר בהסכם) ע"י האגף כלפי הספק במקרים בו התגלה פער במילוי ועמידה בדרישות ההסכם בנושאי אבטחת מידע.

לגבי יתר התגובה של האגף: ההצהרות לשיפורים שהאגף יבצע אינן מלוות בלוח זמנים.

# 18.ביקורות תקופתיות

## 18.1. בקשת נתונים

הביקורת ביקשה נתונים מהאגף בנושא זה כר"מ:

האם בוצעו / מבוצעות ביקורת תקופתיות (פנימיות או חיצוניות) לבדיקת עמידת המאגרים בדרישות החוק והתקנות לאבטחת הפרטיות? אם כן נבקש תיעוד.

## 18.2. נתוני האגף

### 18.2.1. <u>רשימת הנתונים שהתקבלו</u>

נתקבלו מהאגף נתונים לבקשת הביקורת כדלקמן:

1. באוג' 2018 בוצע סקר סיכונים נרחב ע"י חברת MadSec Security
2. בשלהי 2019 התבצעה בדיקת אבטחת מידע ביוזמת המנכ"ל, בסיוע של חברה אבט"מ חיצונית (יש העתק בהארד-קופי).
3. באוג' 2020 הסתייענו ביועץ חיצוני (איש ciso) לביצוע בקרות, בדיקות והמלצות- מצ"ב תוצרי עבודתו.
4. אנו נמצאים בתהליך יציאה למכרז לביצוע סקר סיכונים ומבדקי חדירות, מצ"ב תכולה מתוכננת.

### 18.2.2. <u>התייחסות הביקורת</u>

(1) סקר סיכונים: ראה פרק 9. לעיל

(2) בדיקת אבטחת מידע ביוזמת האגף : לא התקבל מעבר להצהרת האגף כל תיעוד. מבחינת הביקורת אין להצהרה זו, משמעות מעשית מבחינת מענה לבקשתה.

(3) הבדיקה שנערכה באוג' 2020 ע"י היועץ החיצוני מציגה מצד אחד שורה של כ- 30 פערים, ליקויים, וכשלים במרבית נושאי התוכן של אבטחת המידע באגף, אשר תומכים בחלקם הניכר את ממצאי הביקורת. הדוח למעשה מוכיח היעדר פעילות מתקנת או איטיות בלתי תקינה ביישום פעילות מתקנת, אך מצד שני מנסח שורה של המלצות מעשיות אשר להבנת הביקורת האגף החל ביישום של חלק מהם ולמסקנת הביקורת יש לראות זאת בחיוב.
לפירוט ממצאי הבדיקה ראה נספח כ"ו

**(4)** <u>סקר סיכונים ומבדקי חדירות:</u> הביקורת רואה מצד אחד בחיוב התארגנות לביצוע סקר סיכונים ומבדקי חדירות.
מצד שני התמשכות כה ארוכה של ההתארגנות לעריכתו מהווה למסקנת הביקורת ליקוי מהותי ובנוסף הפרת תקנות הגנת הפרטיות. (על אף שאירועי הקורונה יכולים להיחשב

כנסיבות מקילות במידה מסוימת).

לתפיסת הביקורת ולמסקנתה הליך ההתארגנות והביצוע של סקר סיכונים תקופתי (כאמור, עפ"י חוק, בתדירות שלא תפחת מאחת ל- 18 חודש) צריכים להיות מהירים וזריזים לעומת המצב כיום, שההתארגנות איטית מאד ומסורבלת. לתפיסת הביקורת על האגף להתארגן ולהכין תשתית חזקה להוצאה לפועל של סקר כזה, בהליך כמעט סטנדרטי ומבוסס על מערך מוכן מראש ( ומנוהל ומתוחזק) של נושאים ומידע שנדרשים ל"הפקת" האירוע. אבל בכך לא די. לתפיסת הביקורת נדרש להיות ערוך ומוכן עם תשתית הולמת כמו נוהל מחייב והליכי גיבוש תכנון ובקרה לפעילות מתקנת בעקבות הסקר והמבדק ולבדיקת אפקטיביות הפעילות המתקנת. **כל אלו אינם היום בנמצא ויש בהיעדרם למסקנת הביקורת ליקוי מהותי וחמור, בניהול נושא אבטחת המידע.**

**הביקורת ממליצה לתקן ללא דיחוי את הליקויים הנ"ל**

## 19.גיבוי ושחזור נתונים

לבקשת הביקורת הועברו לביקורת 5 נהלים העוסקים בנושא של גיבוי ושחזור נתונים. מתוכם נוהל אחד שמקורו בשנת 2014 ועודכן ב- 2018 ואילו יתר 4 הנהלים אינם נושאים כל תאריך (תופעה שהביקורת כבר עמדה עליה ורואה אותה כליקוי מהותי). יש בנהלים אלו בכדי לספק את בקשת הביקורת לנתונים. עם זאת אין בידי הביקורת כל תיעוד ביחס ליישום נהלים אלו, אשר לפחות חלקם עומדים בכפילות ובחוסר תיאום בהוראותיהם.

19.1.**תגובת האגף לטיוטת דוח הביקורת והתייחסות הביקורת**

19.1.1. **תגובת האגף**

**14.אבטחת מידע/גיבויים**

בעירייה מוטמע שרת גיבוי בבניין נפרד המקושר בסיב אופטי פרטי לשרת הראשי ומשם מבוצעות כמה רמות גיבוי ובין היתר גיבוי ארכיון ורפליקות:

- רפליקציה יומית ושבועית
- גיבוי מלא
- Images

טכנולוגית הגיבוי בה משתמשת העירייה הינה VEEAM, אשר מבצע גם בדיקות אוטומטיות.

19.1.2.**התייחסות הביקורת**

תגובת האגף לטיוטת דוח הביקורת מהווה מענה מניח את הדעת לנושא.

# 20.תוכנית ותרגול להתאוששות מאסון

## 20.1.בקשת נתונים

הביקורת ביקשה נתונים מהאגף בנושא זה כר"מ:

1. האם קיימת תכנית מעודכנת להתאוששות מאסון והמשכיות עסקית ? אם כן נא להמציא תיעוד.
2. האם קיים אתר גיבוי? אם כן להמציא תיעוד.
3. האם מתבצעים ומתועדים תרגולי התאוששות מאסון ומעבר לסביבת הגיבוי. אם כן נא להמציא תיעוד מהשנים 2019 עד 2021.

## 20.2.נתוני האגף

### 20.2.1. <u>רשימת הנתונים שהתקבלו</u>

| נושא | בקשת נתונים ע"י הביקורת | נתוני האגף |
|---|---|---|
| תוכנית ותרגול להתאוששות מאסון | 1. האם קיימת תכנית מעודכנת להתאוששות מאסון והמשכיות עסקית ? אם כן נא להמציא תיעד. | לא |
| | 2. האם קיים אתר גיבוי? אם כן להמציא תיעוד. | מערכת המחשוב עובדת שוטף מ2 אתרים פיזיים. Stretch Cluster מרכזיה טלפונים מגובה באתר ה3 בנוסף |
| | 3. האם מתבצעים ומתועדים תרגולי התאוששות מאסון ומעבר לסביבת הגיבוי. אם כן נא להמציא תיעוד מהשנים 2019 עד 2021. | |

## 20.3.התייחסות הביקורת

### 20.3.1. <u>קיום תוכנית התאוששות</u>

היעדר תוכנית להתאוששות מאסון והמשכיות עסקית מהווה למסקנת הביקורת ליקוי מהותי וחמור.

הביקורת ממליצה לפעול בהקדם לתיקון ליקוי זה ולהיערכות הולמת לתוכנית כזו.

### 20.3.2. <u>אתר גיבוי</u>

תשובת האגף מניחה את הדעת.

20.3.3. **<u>תרגילי התאוששות</u>**

מחוסר ההתייחסות של האגף הביקורת מסיקה כי אין ולא מתבצעים תרגילי התאוששות. הביקורת רואה בהיעדרם ליקוי מהותי.

הביקורת ממליצה לתקן ליקוי זה בהקדם.

20.4.**תגובת האגף לטיוטת דוח הביקורת והתייחסות הביקורת**

20.4.1. **תגובת האגף**

**13.סעיף 20 - תכנית ותרגול להתאוששות מאסון**

תכתב תכנית התאוששות מאסון הכוללת התייחסות לנתוני RPO ו RTO.

יבוצעו תרגולים בהתאם.

20.4.2.**התייחסות הביקורת**

הצהרות האגף לטיוטת דוח הביקורת בדבר פעילות שתיעשה בעתיד, לתיקון הליקויים שהביקורת מצאה וכיישום המלצותיה, אינן מלוות בלוח זמנים.

# 21.תוכניות עבודה לעניין אבטחת מידע

## 21.1.**תוכניות שהתקבלו**

הביקורת קיבלה מהאגף 4 תוכניות עבודה בקבצי אקסל:

21.1.1. **<u>"תכנית עבודה 2020 - אבטחת מידע וסייבר"</u>**

בתוכנית זו מתוכננות פעילות לטיפול ולפעילות מתקנת ב- 34 נושאי אבטחת מידע. טורי התוכנית כוללים את הנושא, את האחראי לביצוע, את סטאטוס הטיפול , לו"ז לבקרת סטאטוס.

למסקנת הביקורת – ללא קשר למידת היישום של התוכנית שהינה נמוכה (רק 8 טופלו וטופלו חלקית) – התוכנית עצמה תקינה ומניחה את הדעת מבחינת תוכנה והתנהלותה. (הביקורת מתרשמת כי התוכנית עברה בקרה למידת יישומה).

21.1.2. **<u>תוכנית ליישום סקר סיכונים משנת 2018.</u>**

גם תוכנית זו מבחינת תכולתה, המבנה שלה והבקרה שנערכה, מניחה את הדעת.

(למרות שרמת היישום בפועל, של סעיפי התוכנית ירודה מאד).

21.1.3. **<u>תוכנית לפעילות מונעת ומתקנת לאירוע אבטחת מידע שהתרחש בעירייה ( במרץ 2020)</u>**

גם תוכנית זו מבחינת תכולתה, המבנה שלה והבקרה שנערכה, מניחה את הדעת.

(למרות שרמת היישום בפועל, של סעיפי התוכנית ירודה מאד).

21.1.4. **<u>תוכנית עבודה - דוח אבטחת מידע</u>**

כמו ב- 3 התוכניות הקודמות

התייחסות הביקורת לנושא תוכניות עבודה

לעניין תוכניות העבודה בנושא אבטחת מידע - רואים כי באגף ערכו תוכנית שנתית אחת ובנוסף מספר תוכניות אקראיות אל מול אירועי שהתרחשו.

לתפיסת הביקורת על האגף להכין מדי שנה בשנה, תוכנית עבודה ברזולוציית בקרה של אחת לרבעון ולנהל ולבקר מידת ביצוע מול תכנון.

בפועל אין תוכניות כאלו ואין בקרה כזו (זולת התוכנית לשנת 2020). הביקורת רואה בכך ליקוי מהותי. וממליצה לפעול בהקדם לתיקונו.

מסקנה זו של הביקורת תואמת למסקנת והמלצות דוח סטטוס אבטחת מידע מ-08/08/2020 (נספח כ"ז)

"לא הוצגו תוכניות עבודה כנדרש בתקנות מאגרי המידע , לא הוצגו תוכניות עבודה בתחום ה SYSTEM , תקשורת וטלפוניה. מנהל ה SYSYTEM ומנהל התקשורת המשמש גם מנהל אבטחת המידע בארגון יציגו כל אחד בתחומו תוכניות עבודה לשנת 2020 ולשנת 2021 , תוכנית העבודה תעמוד בתקנות אבטחת המידע , תהיה מבוססת תקציב או QUICK WINS ".

# 22.סיכום מסקנות

22.1. נמצאו פערים, חריגים וליקויים בניהול הנהלים בנושא אבטחת מידע.

22.2. קיים מסמך מדיניות אבטחת המידע, אבל איננו מתעדכן. אין ניהול של המדיניות.

22.3. במבנה הארגוני קיימים פגמים בהקשר של אבטחת המידע. בנוסף אגף מערכות מידע, לא מופיע כלל באתר האינטרנט של העירייה.

22.4. מונה ממונה אבטח מידע מאגרי המידע כנדרש בתקנות, אך זאת רק לתקופה קצרה של כחודשיים. קיימים ליקויים בהגדרת תפקידו. הממונה הינו ספק חיצוני.

22.5. נשכר מנהל אבטחת מידע שימלא גם את תפקידי ממונה אבטחת מידע בהיקף משרה של 35%. היקף משרה זה תמוה בייחוד בהשוואה למכרז שנתיים קודם, למנהל אבטחת מידע בהיקף של משרה מלאה. שכירת ממלא תפקיד זה נעשתה חרף קיומו של מנהל אבטחת מידע באגף (המקבל גם ביטוי בתרשים המבנה הארגוני).

22.6. נמצאו ליקויים בהליכי הבחירה של מנהל אבטחת מידע (שממלא גם תפקידי ממונה אבטחת מידע). (ספק חיצוני)

22.7. וועדת היגוי לא סדירה מבחינת הגדרת צוות הוועדה וכמעט שלא התכנסה ב-3 השנים האחרונות.

22.8. נמצאו ליקויים מהותיים בניהול מאגרי המידע בעירייה.

22.9. סקר הסיכונים שבוצע ביולי 2018 הצביעה על רמת סיכון גבוהה, בהיבט אבטחת המידע ואיומי חדירה. חלק ניכר מהמלצות סקר סיכונים לשנת 2018 להפחתת הסיכונים המשמעותיים (הבלתי קבילים) לא יושם. אין מבצעים סקרי סיכונים בתדירות הנדרשת בחוק - לפחות פעם ב-18 חודש. נכון לתקופת הביקורת סקר הסיכונים האחרון שבוצע היה ב 2018.

22.10. אבטחה פיזית וסביבתית של מאגרי המידע - נמצאו ליקויים ופערים בעיקר בתחום הנהלים, המודעות וההדרכה. באחד מחדרי השרתים נמצאו ליקויים מהותיים וחמורים, בתחום ההגנה נגד אש וגיבוי לנפילת חשמל.

22.11. באבטחת מידע לניהול כ"א והרשאות, חלק מהיבטי הנושא מנוהלים באופן תקין וחלקו סובל מליקויים מהותיים.

22.12. הדרכות בנושא אבטחת מידע - נמצאו פערים מהותיים בניהול הנושא.

22.13. אירועי אבטחת מידע - היו ב-3 השנים האחרונות לפחות 2 אירועים מדווחים. אחד מהם תוך פגיעה משמעותית. לדברי הנהלת האגף, בתגובתה לטיוטת דוח הביקורת, האירועים תוחקרו

וטופלו. כמו כן, לדבריה, נוהל טיפול באירוע מטוייב בעת האחרונה ומוסדר גם נושא התחקירים. תגובת הנהלת האגף הינה ללא תיעוד כסימוכין וללא לו"ז לביצוע.

22.14. אבטחת מידע התקנים ניידים – הועבר לביקורת נוהל גנרי לנושא, שאיננו נושא לוגו כלשהו. לא הוצג כל תיעוד לגביי פעילות מניעה, בקרה וכיו"ב, ביחס לטיפול האגף בנושא. לדברי הנהלת האגף, בתגובתה לטיוטת דוח הביקורת, " הנושא טופל ע"י אנשי אגף מערכות המידע במרץ 2020 . " תגובת האגף איננה מלווה בתיעוד כלשהו כסימוכין .אבטחת מידע בהתקשרות עם ספקי שירותי מערכות מידע - נמצאו ליקויים ופגמים רבים ומהותיים.

22.15. תוכניות ותרגול להתאוששות מאסון - נמצאו ליקויים מהותיים ופערים בניהול הנושא.

22.16. תוכניות עבודה לעניין אבטחת מידע – נמצאו מצד אחד תוכניות מניחות את הדעת כתגובה לצרכים מקומיים ומצד שני פערים לעניין תוכניות עבודה שנתיות.

## 23. המלצות

לתקן את הליקויים, הפגמים והפערים שנמצאו בביקורת כהמלצות הביקורת. דגש מיוחד על:

סקר סיכונים, פעילות מתקנת ומונעת לאירועי חדירה, ניהול מאגרי המידע.

## 24. התייחסות מסכמת של הנהלת האגף לטיוטת דוח הביקורת

**סיכום**

ניהול נושא אבטחת המידע והגנות הסייבר עובר מאז מתקפת הסייבר שינוי מהותי, הן בהיבטי המבנה הארגוני, הן בנושאי בקרות טכנולוגיות והן בנושאים ניהוליים בתחום. בנוסף עורך האגף מיפוי מלא בכל הכרוך בסיכוני סייבר ומבצע סקר באמצעות חברה חיצונית. האגף מאמין כי בביקורת הבאה חלק ניכר מן הנושאים המצוינים בדוח זה יטופלו.

# נספחים

## נספח א' - דוגמת נוהל מקבוצת נהלים א'

נוהל לדוגמה מקבוצה א'

| | | | |
|---|---|---|---|
| **עיריית הוד-השרון** | | **נוהל "אבטחת מידע"** | **מספר הנוהל:**<br>**026– 100000 – 1029** |
| **מהדורה:** | **002** | **תאריך תחולה:** | **עמוד** 46 **מתוך** 112 |
| **הפרק:** | **אבטחת תפעול מערכות מידע** | | **עותק מספר:** |
| **הנושא:** | **תפעול חדר מחשב** | | **מתוך:** |

1.כללי

1.1.תפעול מסודר ומבוקר של חדר ההפעלה מהיבט של אבטחת ענ"א.

2.הגדרות

2.1.חדר המחשב - אולם ההפעלה בו מוצבים מחשבי העירייה והנמצא במבנה יחידת המחשוב בעירייה.

3.מטרה

3.1.לא לאפשר סיכון הציוד והמידע כתוצאה ממפגע מזדמן או אירוע חריג בלתי מבוקר.

3.2.לפקח ולבקר אבטחתי את הפעילות בחדר ההפעלה.

4. אסמכתאות וזיקות

4.1. אין.

5.שיטה

5.1. חדר המחשב יהיה נעול בכל עת.

5.2. בתוך חדר המחשב, יורשו להימצא בשגרה ולצורך ביצוע עבודתם: מפעילי המחשב, מנהל מערכות מידע, אנשי תחזוקה בליווי המורשים.

5.3.יורשו לאשר חריגים: מנהל מערכות מידע.

6. ייזום נהלים.

7. אמצעים.

8. אחריות.

8.1. מנהל מערכות מידע אחראי לביצוע הנוהל.

9.נספחים.

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

## נספח ב' - דוגמת נוהל מקבוצת נהלים ב'

אושר על ידי מנכ"ל העירייה ביום 18.11.07

# נוהל פנימי

# בירור ו/או איסוף מידע ממחשבים של העירייה המצויים בשימוש עובדיה

### מטרת הנוהל

1. להבטיח כי כל החלטה בדבר חדירה למחשב שבו משתמש עובד עירייה לצורך בירור ו/או איסוף מידע – תעשה באופן ענייני, תוך בחינת כל השיקולים הרלוונטיים, וכן כי היא תתקבל באופן מידתי וסביר על פי נסיבות הענין.

### הגדרות

2.

2.1 "מחשב" – "חומר מחשב" ו – "תוכנה" כהגדרתם בחוק המחשבים, התשנ"ה – 1995.

2.2 "רשומות מחשב" – מידע שבמאגר הממוחשב של העירייה.

### הצוות הממונה על טיפול בבקשות לפי הנוהל וקבלת החלטות לשימוש במידע הנאסף – הרכב ותפקידים

3. ראש העיר ימנה צוות לטיפול בבקשות לפי נוהל זה.

4. הצוות ימנה 3 חברים: מנכ"ל העירייה, היועץ המשפטי וחבר נוסף שימונה על ידי ראש העיר.

5. תפקידו של הצוות הממונה לדון בבקשות, לאשרן ו/או לדחותן, באופן מלא או חלקי. בנוסף, ואם החליט הצוות הממונה להורות על בירור ו/או איסוף מידע שהופק ממערכת המחשוב, והמידע כאמור נאסף, ישוב הצוות הממונה וידון במידע שנאסף ויורה על דרכי השימוש בו על פי המטרה שלשמה נאסף.

**<u>הגשת בקשות לבירור ו/או איסוף מידע ממוחשב</u>**

6. בקשה לפי נוהל זה יכול שתהא מוגשת אך ורק על ידי ראש העירייה, מנכ"ל העירייה ומנהל אגף בעירייה. הבקשה תוגש למנכ"ל העירייה בכתב ותפרט את תוכן המידע המבוקש ומטרתו.

7. מצא מנכ"ל העירייה, כי יש ממש בבקשה, הוא יורה על זימונו של הצוות הממונה.

**<u>דיון הצוות הממונה בקשה</u>**

8. הצוות הממונה יקיים דיון בבקשה והוא רשאי לזמן את הגורם המבקש לקבלת הסברים ו/או הבהרות. הגורם המבקש יתייצב בפני צוות הבדיקה וזאת כתנאי להמשך בירור בקשתו.

9. הצוות הממונה יבחן את הבקשה, את נחיצות המידע המבוקש, את תכלית השימוש בו וכן יהא רשאי לשקול כל ענין אחר רלוונטי - הכל בהתאם להוראות כל דין.

10. מצא הצוות הממונה כי יש צורך בבירור ו/או באיסוף מידע מבוקש, ייתן החלטתו ונימוקיו בכתב. בהחלטתו יפרט הצוות הממונה את דרך איסוף המידע, יטיל הגבלות ו/או הנחיות מפורטות ויתווה את הדרך לבירור ו/או איסוף המידע שדבר בירורו ו/או איסופו הותר, לרבות מינוי חבר מבין חברי הצוות הממונה שיתלווה לעובד העירייה המקצועי (ו/או אדם שמועסק על ידי העירייה) בעת ביצועו את פעולת הבירור ו/או האיסוף.

11. הצוות הממונה יהיה רשאי לזמן את עובד העירייה, שלגביו ו/או לגבי המחשב שנמצא בשליטתו, מבוקשת הבדיקה.

**<u>קבלת הסכמת העובד</u>**

12. הצוות הממונה יבקש את הסכמת עובד העירייה לביצוע פעולת בירור ו/או איסוף המידע. הצוות הממונה יהיה רשאי, במקרים מסויימים לפי הענין שלא לקבל את הסכמת העובד לביצוע הפעולה כאמור, ובמקרה זה יהיה עליה לפרט בהחלטתה את נימוקיה המיוחדים לכך.

**<u>דיון נוסף</u>**

13. החומר שנאסף ו/או נתונים אחרים שדבר בירורם התבקש על ידי הצוות הממונה, יועברו במעטפה חתומה למנכ"ל העירייה (להלן – המידע שנאסף).

14. לאחר קבלתו את המידע שנאסף, יזמן מנכ"ל העירייה את הצוות הממונה לבחינת המידע שנאסף, וכן לצורך קבלת החלטה באיזה מידע יעשה שימוש ובאיזה אופן.

**<u>תחזוקת מערכות המחשוב והתקשורת</u>**

15. תחזוקה מונעת, תיקונים הוספות ועדכונים טכנולוגיים של מערכות המחשוב והתקשורת יבוצעו באופן סדיר, מהיר ומיומן על ידי טכנאים של ספקי השירות, שאושרו על ידי ראש העירייה ו/או מי מטעמו. ביצוע פעולות אלה ייעשה בלי שתהיה לטכנאים האמורים גישה לתכנים של רשומות מחשב שבמאגר מידע ו/או בכל מחשב בנפרד. במידה שלא ניתן לבצע פעילויות אלה בלי גישה לתכנים כאמור, תעשה הפעילות בפיקוח צמוד של עובד העירייה שימונה לכך על ידי הצוות הממונה.

**<u>שמירת סודיות</u>**

16. כל דיוני הצוות הממונה, לרבות כל מסמך ו/או מידע שהתקבלו במסגרת נוהל זה, יהיו חסויים, ולא ימסר מתוכם כל מסמך ו/או מידע למאן דהוא, אלא בהתאם להחלטות הצוות הממונה.

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

**נספח ג' - דוגמת נוהל מקבוצת נהלים ג'**

**עיריית הוד השרון**

**אגף מערכות מידע**

נוהל אבטחת מידע - אבטחת קלט/פלט - נייר

## כללי

חומר כתוב טרם הקלדתו או תדפיסי/דו"חות מחשב, עלולים להוות מפגעי אבטחה חמורים, אלא אם כן, ננקוט אודותם באמצעי אבטחה נאותים.

## הגדרות

קלט נייר - תעודות למיניהן, טופסי קידוד וכיוצא באלה, המשמשים להזנת נתונים למחשב.

פלט נייר - תדפיסים המופקים במדפסות של מחשב, כגון: דו"חות, גרפים, חשבוניות וכל נייר אשר מכיל נתונים לגבי פעילות העירייה כיוצא באלה.

גריסה - פעולת גריסה המתבצעת במשרדי העירייה, מתאים לכמויות קטנות.

ביעור - העברת תדפיסים להשמדה באופן מאובטח וקבלת תעודת השמדה, מתאים לכמויות גדולות.

נייר למיחזור - ניירות שאין בהם מידע אישי או מידע לגבי פעילות העירייה וניתן להעבירם באופן גלוי למיחזור.

## מטרה

לפרט את סדרי האבטחה שיש לקיים אודות טופסי קלט מחד, ודו"חות/תדפיסי מחשב – מאידך.

## אסמכתאות וזיקות

חוק הגנת הפרטיות.

תקנות הגנת הפרטיות.

## שיטה

<u>סימון וסיווג קלט/פלט</u>:

1.1.1. כל מסמך המוגדר - אישי - , יצוין כך בראש המסמך.

1.1.2. מסמכים המכילים מידע על פעילות העירייה ויש בפרסומם פגיעה בעירייה או באדם יש לטפל במשנה זהירות - לגרוס מיידי או לבער.

<u>טיפול בפלט - מדפסת מרכזית</u>:

1.1.3. פלט המופק במדפסת המרכזית יופק בנוכחות הגורמים המורשים ליד המדפסת ויטופל אך ורק ע"י הגורמים המורשים לפלט.

1.1.4. חומר עודף או לקוי, יישמר נעול ויטופל על ידי יוזם ההפקה כמתואר בהמשך.

1.1.5. פלטי מחשב, יפונו באופן שוטף וימסרו למשתתפים באופן מיידי. חומר שלא יועבר, ישמר בארון נעול עד למסירה.

1.1.6. שימוש חוזר בנייר מחשב שיש עליו נתונים של העירייה לא ישמש לשימוש חוזר כטיוטה.

<u>הפצה</u>:

1.1.7. העברת חומר מסווג תהייה כשהוא ארוז.

<u>פלט אצל משתמשים</u>:

1.1.8. כל פלט מכל סוג, ימצא ויטופל רק אצל המוסמכים לקבלו בהתאם לקביעת מנהל היחידה במקום.

1.1.9. חומר שאיננו בשימוש או לאחר שעות הפעילות הרגילות, יינעל בארונות.

1.1.10. פלט שפג תוקפו או שאין בו צורך, ייגרס במקום או יועבר לביעור באחריות מנהל היחידה.

1.1.11. לא יועבר חומר עם נתוני עירייה למחזור כשהוא בשלמותו ואינו גרוס.

1.1.12. תדפיסי מחשב לאחסון בארכיב, יש לפנות כשהם ארוזים ומסומנים. הפינוי יתבצע ע"י מורשה לחומר, ישירות לארכיב.

1.1.13. חומר מסווג לא יופק במדפסת רחוקה, אלא אם כן יעמוד ליד המדפסת – הגורם המורשה לקבל את החומר.

<u>ביעור והשמדה</u>:

1.1.14. מסמכים, דו"חות מסווגים, שאין בהם צורך יותר, ייגרסו בעירייה או יועברו לביעור באופן שוטף, באחריות מנהל היחידה.

1.1.15. תדפיסים פגומים, מיותרים וכדומה, יש לגרוס באופן מיידי או לבער באחריות המחזיק בהם.

1.1.16. חומר לגריסה לא יישאר ליד המגרסה, אלא אם כן יינעל בארון.

1.1.17. ביעור שוטף של פלטי מחשב באתרי העירייה השונים, יבוצע ע"י העברתו לביעור או גריסה במתקני העירייה.

1.1.18. מסמכים שלא נגרסו לא יושארו בשטח נגיש לציבור, אלא יישמרו במשרד סגור שניתן לנעול, ללא גישה למי שאינו מורשה למידע.

## <u>ייזום נהלים</u>

אין.

## <u>אמצעים</u>

7.1 לצורך ביצוע נוהל זה יש לספק מגרסות בגודל בהתאם לנפח הגריסה לכל יחידות העיריה.

7.2 יש לאפשר פניה לגורם המספק שירותי ביעור תקינים.

7.3 מומלץ לאסוף חומר בקופסאות שונות - חומר לגריסה, חומר לביעור.

## אחריות

אחריות לביצוע נוהל זה חלה בהתאמה על מנהלי יחידות בעירייה ומשתמשים.

באחריות מנהל אבטחת מידע לוודא ולבקר קיומו של נוהל זה.

## נספחים

אין.

## נספח ד' - נוסחי כותרות בנהלים

1) כותרת נוסח 1 - כותרת אחידה

לכמחצית מרשימת הנהלים (לכ-39 נהלים) יש כותרת אחידה בראש כל נוהל כמוצג בדוגמה להלן:

| עיריית הוד-השרון | | נוהל "אבטחת מידע" | מספר הנוהל: 012 – 100000 – 1029 |
|---|---|---|---|
| מהדורה: | 002 | תאריך תחולה: | עמוד 54 מתוך 112 |
| הפרק: | אבטחה בתוכנה | | עותק מספר: |
| הנושא: | זיהוי משתמשים במחשבים מרכזיים | | מתוך: |

למחצית האחרת יש נוסחים שונים לכותרות הנוהל כמו הדוגמאות שלהלן:

2) כותרת נוסח 2 – כבדוגמה

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

**עיריית הוד השרון**

**אגף מערכות מידע**

סימוכין:216939

14/04/2019

נוהל אבטחת מידע - אבטחת קלט/פלט - נייר

3) כותרת נוסח 3 - כבדוגמה

אושר על ידי מנכ"ל העירייה ביום 18.11.07

**נוהל פנימי**

**בירור ו/או איסוף מידע ממחשבים של העירייה המצויים בשימוש עובדיה**

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

4) כותרת נוסח 4 - כבדוגמה

**עיריית הוד השרון**
**אגף מערכות מידע**

סימוכין:216939
14/04/2019

מנה גולן
מנכ"לית
עיריית הוד השרון

נוהל אבטחת מידע - אבטחת קלט/פלט - נייר

**נספח ה'**

| עיריית הוד-השרון | | נוהל "אבטחת מידע" | מספר הנוהל: 1029 – 100000 – 006 |
|---|---|---|---|
| מהדורה: | 002 | תאריך תחולה: | עמוד 57 מתוך 112 |
| הפרק: | אבטחת תקשורת | | עותק מספר: |
| הנושא: | תקשורת – אבטחת תפעול | | מתוך: |

## כללי

אחת מנקודות התורפה הקשות בתחום **אבטחת מערכות המידע**, הינה התקשורת. יש לכך חשיבות רבה בפעילות אבטחתית בתחום זה.

## הגדרות

אין.

## מטרה

להנחות אודות סדרי אבטחה שונים בתחום : תפעול מערכת התקשורת.

## אסמכתאות וזיקות

אין.

## שיטה

השירות הרגיל למשתמשי המחשב, בשעות הפעילות הרגילות של העירייה. שירותי התקשורת פועלים 24 שעות ביממה.

משתמש או כל גורם אחר שיבקש לפעול מעבר לשעות הנ"ל, יפנה במשך שעות הפעילות, ויתאם פעילות חריגה.

פעילות בתקשורת בשעות החורגות מהמקובל, תוגדר כפעילות חריגה, על כל המשתמע מכך.

לאחר 30 דקות של אי-פעולה מהמחשב, יתבצע כיבוי מסך.

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

## ייזום נהלים

| | |
|---|---|
| **אישור מנהל היחידה:** | **תאריך עדכון:** |
| **אישור מבקר פנים:** | **מבטל נוהל מספר:** ---------- |
| **אישור היועמ"ש:** | **מהדורה:** 002 **מתאריך** --------- |
| | -- |
| **אישור מנכ"ל:** | **אישור ממונה נהלים:** |
| **חל על יחידות:** | |

| עיריית הוד-השרון | | נוהל "אבטחת מידע" | מספר הנוהל: 1029 – 100000 – 006 |
|---|---|---|---|
| מהדורה: | 002 | תאריך תחולה: | עמוד 59 מתוך 112 |
| הפרק: | אבטחת תקשורת | | עותק מספר: |
| הנושא: | תקשורת – אבטחת תפעול | | מתוך: |

## אמצעים

## אחריות

מנהל מערכות מידע אחראי על ביצוע נוהל זה.

## נספחים

| | | |
|---|---|---|
| אישור מנהל היחידה: | | תאריך עדכון: |
| אישור מבקר פנים: | | מבטל נוהל מספר: ---------- |
| אישור היועמ"ש: | | מהדורה: 002 מתאריך --------- |
| | | -- |
| אישור מנכ"ל: | | אישור ממונה נהלים: |
| חל על יחידות: | | |

**נספח ו' – מדגם נהלים**

| עיריית הוד-השרון | | נוהל "אבטחת מידע" | מספר הנוהל: 1029 – 100000 – 004 |
|---|---|---|---|
| מהדורה: | 002 | תאריך תחולה: | עמוד 60 מתוך 112 |
| הפרק: | אבטחה פיסית ובטיחות | | עותק מספר: |
| הנושא: | בקרת כניסה ליחידת המחשב | | מתוך: |

## כללי

אבן יסוד בכל פעילות לאבטחה מערכתית, הינה פעילות בתחום בקרת הגישה הפיסית.

## הגדרות

אזור יחידת המחשב – חדר המחשבים.

## מטרה

לקבוע את סדרי הבקרה והכניסה לאזור חדר המחשב המרכזי והשרתים – בעירייה.

## אסמכתאות וזיקות

נוהל כניסה מבוקרת.

## שיטה

הכניסה לאזור יחידת המחשב תהיה מבוקרת ותותר לעובדי היחידה ולגורמים נוספים, מורשים בלבד.

חדר המחשב יהיה נעול באופן קבוע. עובד מורשה יוכל להיכנס לחדר לביצוע תפקידו בלבד.

המחשב המרכזי יהיה מוצב בחדר בעל קירות מבנייה קשה, ללא פתחים פרט לדלת כניסה. דלת הכניסה תהיה מסוג "רב-בריח" עם נעילה תואמת.

אורחים בלתי קבועים יהיו רשאים להיכנס על פי אישור מנהל מערכות מידע או גורם מוסמך אחר.

באחריות הגורם המארח, לדאוג לכך שהאורחים לא יסתובבו באזור המחשב שלא לצורך. עם סיום ביקורם, ילוו האורחים אל מחוץ לאזור.

אורח המגיע ללא תיאום, ייבדק הצורך בכניסתו עם הנוגע בדבר, ואזי תותר כניסתו בכפוף למפורט לעיל אודות אורח.

| | |
|---|---|
| **אישור מנהל היחידה:** | **תאריך עדכון:** |
| **אישור מבקר פנים:** | **מבטל נוהל מספר:** ---------- |
| **אישור היועמ"ש:** | **מהדורה:** 002 **מתאריך** --------- |
| | -- |
| **אישור מנכ"ל:** | **אישור ממונה נהלים:** |
| **חל על יחידות:** | |



דלת הכניסה לחדר המחשב תהיה סגורה בכל עת, רשימת. מנהל מערכות מידע יהיה המוסמך לאשר הרשימה והחריגים.

## ייזום נהלים

נוהל זה תקף עם פרסומו.

## אמצעים

## אחריות

מנהל מערכת מידע, אחראי לקיום נוהל זה. באחריותו כוחו לבקר באופן שוטף את המצב.

## נספחים

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

**נספח ז' - מדיניות אבטחת מידע**

**עיריית הוד השרון**
**אגף מערכות מידע**

# מדיניות אבטחת מידע ונהלים

## תקציר מנהלים

מסמך זה מפרט את מדיניות אבטחת המידע של **עיריית הוד השרון** (להלן "**הארגון**") כפי שגובשה ואושרה ע"י הנהלת הארגון.

בשל תחום עיסוקו של הארגון והוראות חוק החלות על פעילותו, קיימת חשיבות עליונה לכך שפעילות הארגון תתבצע תוך עמידה בקריטריונים נאותים והולמים של אבטחת מערכות המידע בכלל ושמירה על חיסיון המידע בפרט, בשקיפות, באיזון ושמירה על טוהר המידות.

מטרתו של מסמך זה לספק הכוונה ותמיכה להנהלת הארגון בנושא עקרונות אבטחת המידע ושמירה נאותה של המידע האישי ונכסי המידע בארגון .

על עקרונות אלו להתייחס לנושאים כגון שימוש ברשת האינטרנט ובדואר אלקטרוני, שמירה וטיפול במידע כולל סיווג מסמכים, הרשאות גישה לוגיות ופיזיות, שמירה ושימוש בסיסמאות, שימוש במדיה נתיקה ('דיסק און קי', אפליקציות שיתוף קבצים וכו'), נעילת המחשב בפני גישה כאשר אינו בשימוש, קליטה של מערכות מידע חדשות או בעת שדרוג מהותי של מערכות מידע קיימות, התקשרויות עם גורמי חוץ וכדומה .

ביצוע ויישום מדיניות זו מוגדרים על ידי הנהלת הארגון כיעד אסטרטגי של הארגון כחלק משמירה על חיסיון המידע אשר מוגדרת כמרכיב מהותי ומוביל בתפיסה הניהולית של הארגון.

יישום ההוראה הינו תהליך מורכב הדורש תכנון קפדני בהתאם לאופי הארגון. לשם יישום ההוראה, יכתבו וייושמו נהלי עבודה המבוססים על מסמך המדיניות שאושר ע"י הנהלת הארגון ותבוצע בדיקה שגרתית בעזרת סקרי סיכונים ומבדקי חדירה.

מדיניות זו חלה על כל עובדי הארגון, ספקים ושותפים עסקיים בפעילותם במערכות הארגון.

הארגון יישם מגוון אמצעים לאבטחת מידע על כלל נכסי המידע ולכל נכס ונכס, בהתאם למידת הנזק העשויה להיגרם לארגון כתוצאה מכשל באבטחת נכס המידע וההסתברות לקרות אירוע הכשל.

על החתום:

10.3.19 — איריס כהן, מנהלת מערכות מידע, עיריית הוד השרון, מנכ"ל

10/3/19 — חנה עולין, מנכ"לית, עיריית הוד השרון, מנכ"ל

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

**עיריית הוד השרון**
**אגף מערכות מידע**

## 1. עקרונות מדיניות אבטחת מידע

אבטחת מידע היא שמירה על עמידות המידע בתנאים הבאים:

- **חיסיון וסודיות** (**Confidentiality**) – וידוא שהמידע נגיש רק למי שקיבל הרשאת גישה.
- **שלמות (Integrity)** – שמירת הדיוק והשלמות של המידע ושיטות עיבודו.
- **זמינות (Availability)** – וידוא שלמשתמשים מורשים יש גישה למידע ולנכסים הקשורים בו, לפי הצורך.

## 2. מטרות אבטחת המידע

מטרותיה של אבטחת המידע בארגון מפורטות להלן:

- למזער את הסיכון הכלכלי הכרוך בכשלי אבטחת מידע בפעילות הארגון.
- לאפשר עמידת הארגון בדרישות החוק, רגולציות והתקשרויות חוזיות החלות עליו.
- לאפשר לארגון לעשות שימוש מיטבי במידע בשני אופנים:
  - חיובי – אפשור שיתוף מידע ברמה גבוהה לכל מי שמורשה לכך לקידום מטרות הארגון.
  - שלילי – מניעת שימוש במשאבי המידע של הארגון על ידי גורמים זרים או עוינים מבית ומחוץ.
- מניעת זליגת מידע.
- הבטחת ההמשכיות העסקית של הארגון.

## 3. תיחום היישום של אבטחת מידע

אבטחת המידע תיושם על כל נכסי המידע של הארגון: נתונים, תהליכי עבודה (כולל תהליכים תפעוליים וניהוליים), מערכות, פלטפורמות, אנשים, מידע וידע המאוחסנים באמצעים שונים – אלקטרוניים, פיסיים או אנושיים אשר זוהו כבעלי ערך לארגון .

## 4. הצהרת כוונות ההנהלה

הנהלת הארגון מצהירה בזאת כי קביעת מדיניות אבטחת מידע הולמת לארגון ויישומה בפועל בכל פעילויות הארגון הינה יעד אסטרטגי של הארגון, וכי היא מחויבת באופן שאינו משתמע לשני פנים לתהליך זה. כפועל יוצא מכך, הנהלת הארגון תקצה את המשאבים הנדרשים על מנת להביא את הארגון לתפקוד תחת מדיניות אבטחת המידע שהוגדרה במסמך זה.

## 5. תחולת המדיניות

מדיניות זו תחול על כל עובדי הארגון בפעילותם בארגון ו\או במסגרת הארגון. בנוסף, תוחל מדיניות זו גם על גורמים מחוץ לארגון, כגון קבלני משנה, ספקים וארגונים נוספים אחרים השותפים בפעילות הארגון.

# 6. עקרונות המדיניות

## 6.1. מקורות הדרישה לאבטחת מידע

### 6.1.1. הקטנת הסיכון

הקטנת הסיכון תתקיים על ידי יישום מנגנוני אבטחת מידע בארגון וזאת כחלק מהכרתו של הארגון כי פעילותו נוגעת בפן האישי הפיננסי והחסוי, כל זאת מחייב יישום אמצעי אבטחת מידע הולמים על מגוון נכסי המידע שברשות הארגון. יישום נכון של אבטחת מידע תקטין את החשיפה הנזיקית של הארגון ותעלה את קרנו בעיני ציבור המשתמשים והלקוחות .

המטרה הקטנת הסיכון, עד לכדי כך שהסיכון השיורי יהיה קביל ע"י הנהלת הארגון.

### 6.1.2. התאמה לדרישות על פי דין

על הארגון חלות הוראות ספציפיות כגון חוק הגנת הפרטיות התשמ"א-1981, תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז–2017 ואף דרישות חוזיות אחרות כפי שהארגון יתבקש אל מול שותפיו העסקיים\תפעוליים והתושבים. על הארגון לנקוט בכל האמצעים העומדים לרשותו לצורך עמידה בדרישות אלו.

## 6.2. שיטת גיבוש מדיניות אבטחת המידע

גיבוש מדיניות אבטחת המידע בארגון הוא תהליך סיסטמתי המכיל את השלבים הבאים:

### 6.2.1. זיהוי נכסי המידע

בתהליך זה תוגדר אחריות מיפוי הנכסים בצורה מדויקת, תוך מתן תיאור מפורט של נכס המידע ואמצעי האחסנה, הגישה, הגיבוי, האבטחה, קבוצות המשתמשים ומנהל הנכס. משנקבעו כללים לגבי תהליך גיבוש ההערכה למידת החיסיון, כלילות וזמינות נכסי המידע ייקבע בעל הנכס אשר ישמש האחראי על ניהול הנכס בפעילות השוטפת של הארגון.

### 6.2.2. הערכת רמת הקריטיות של נכסי המידע שזוהו

לגבי כל נכס מידע שיזוהה, יגובשו כללים לקביעת רמת הקריטיות שלו במסגרת פעילות הארגון, וכל זאת בהתבסס על המידע שנאסף על נכס המידע בתהליך הזיהוי, הקריטריונים יהיו אחידים לכל נכס מידע באותו סיווג.

### 6.2.3. הערכת סיכוני אבטחת המידע לנכסי המידע וסיכויי התממשותם

לאחר בדיקת נכסי המידע כפי מצבם העדכני, תבוצע הערכה אובייקטיבית של הנזק האפשרי כתוצאה מכשלי אבטחת מידע שונים (דוגמת שריפה, השמדה, גניבה וכו'), בהתאם לרמת הקריטיות של נכס מידע מסוים והערכת סיכויי ההתממשות של כשל זה. מכפלת הערכת הנזק בסיכויי התממשותו מסווגים את מידת הצורך ביישום אמצעי אבטחת מידע, או שיפורו, בהיבט הכשל הספציפי.

### 6.2.4. ניהול הסיכונים לנכסי המידע

על בסיס התהליכים הקודמים, מתוקצבים ומיושמים הפתרונות ומנוהלים הסיכונים לנכסי המידע. מיושמים פתרונות אבטחת מידע, בקרות, רישום וניתוח הכשלים שאירעו, וכמו כן מעקב אחר שינויים בהערכת הסיכונים .

**6.2.5. מיפוי גורמי הצלחה הקריטיים לבחינת מדיניות אבטחת המידע**

לכל נוהל הנגזר ממדיניות אבטחת המידע יקבעו פרמטרים לבחינת הצלחת המדיניות (במסגרת האפשר), באמצעות גורמי הצלחה שיזוהו כקריטיים, תימדד הצלחתה או כישלונה של מדיניות אבטחת המידע של הארגון.

**6.3. הכלים למימוש אבטחת מידע**

על מנת להביא את הארגון לרמת אבטחת מידע נאותה נעשה שילוב בין שלוש קבוצות אמצעים:

**6.3.1. בקרות טכנולוגיות**

ייושמו בקרות טכנולוגיות כנדרש ברמת החומרה, התוכנה והתקשורת, כגון הצפנה, תוכנות אנטי-וירוס, חומת אש, פתרון הגנה על בסיסי נתונים ופתרונות למניעת זליגת מידע, פתרון לניהול ובקרה על מבואות התקשורת (NAC) ומערכת אירועי אבטחת מידע, מערכת לניטור, גיבוי ועוד. כל אלו ייושמו באופן מקיף ולאחר שיקול מעמיק על כל נכסי המידע החשובים של הארגון.

**6.3.2. בקרות פיסיות**

ייושמו אמצעים פיסיים, כגון חדר שרתים מאובטח פיזי, מערכות לניטור ובקרה, תגי זיהוי עבור עובדים, יועצים, עובדי מיקור חוץ ועוד אשר נדרשים לביקורים תדירים בעירייה.

**6.3.3. בקרות ניהוליות**

ייושמו בקרות ניהוליות כגון נהלי עבודה מחייבים ויישומם בכל היבטי העבודה הרלוונטיים לנושא אבטחת מידע, ומנגנון של הטלת האחריות על מנהל הנכס לאבטחת המידע על הנכס שבבעלותו ומתן סמכות לפעולה בתחום האחריות התואמים את דרישות החוק.

**6.4. אחריות וסמכות**

יוגדר מנהל לכל נכס מידע בארגון. על מנהל הנכס תוטל האחריות לאבטחת המידע של הנכס שבניהולו, ותוקנה לו הסמכות הניהולית לבצעה.

בסמכותו של מנהל אבטחת המידע (מדווח ישירות למנמ"ר), נמצאים כל הנושאים התפעוליים הקשורים באבטחת המידע בארגון והוא משמש גם כיועץ למנהלי הנכסים בכל הנוגע לאבטחת המידע של הנכסים שבבעלותם. בנוסף, הוא אחראי להגדרה וביצוע תהליכי בקרת אבטחת מידע ויצירת מנגנון לזיהוי של שינויים בסביבה העסקית של הארגון המחייב שינוי בכללים.

כמו כן, תוגדרנה 'וועדת היגוי לאבטחת מידע', שתפקידה לדון בנושאים הקשורים בנושאי ואירועי אבטחת מידע ופרטיות, ולאשר פרויקטים ברמה הרוחבית\אסטרטגית בארגון,
ו-'וועדה למסירת מידע' שתפקידה לדון בבקשות לקבלת מידע הן של גופים ציבוריים והן של גופים פרטיים.

<u>הערה</u>:
וועדת ההיגוי, מנהל אבטחת המידע, ומנהלי המידע יהוו את הסמכות המקצועית והניהולית לטיפול בכלל הנושאים הקשורים לשמירה נאותה על פרטיות ואבטחת כלל נכסי המידע בארגון.

**6.5. הדרכה**

הטמעתה של מדיניות אבטחת המידע תשולב במערך ההדרכה של עובדי הארגון. הדרכת נוהלי העבודה, כמו גם השימוש בכלים המשמשים לאבטחת מידע הינם חלק בלתי נפרד מתהליך ההכשרה והעבודה בארגון.

**6.6. אמצעי משמעת (אכיפה)**

עמידה ביעדי מדיניות זו ובנוהלי העבודה הנגזרים ממנה הוא תנאי ממכלול ההעסקה של עובד בארגון. וועדת היגוי לאבטחת מידע תידון ותחליט על אופן הטיפול באי עמידה בהוראות מדיניות זו או, בנוהל הנגזר ממנה.

**6.7. הקצאת משאבים**

הארגון יישם לכל נכס מידע שיזוהה כערכי, אמצעים טכנולוגיים, פיזיים וניהוליים ההולמים את מידת חשיבותו בפעילות הארגון. נהלי העבודה מתייחסים לכל שלבי מחזור החיים של עובד בארגון– מיון, קליטה, הכשרה, עבודה ועזיבה, ולכל מחזור החיים של המידע – יצירה, שימוש, אחסון, תחזוקה והשמדה.

**6.8. המשכיות עסקית והתאוששות מאסון**

הארגון מהווה גוף שפעילותו המרכזית מתבצעת באמצעים אלקטרוניים דיגיטליים. מחד גיסא הוא חשוף לסכנה שפגיעה בלב המערכות של הארגון תנטרל את הפעילות כליל. מאידך גיסא, יישום נכון של אמצעי גיבוי ותוכנית להתאוששות מאסון (DRP) אפשריים יבטיחו את ההמשכיות העסקית של הארגון.

מדיניות זו מכריזה גם כי השמירה על המשכיות העסקית היא מיסודות אבטחת המידע של הארגון.

## 7. סיכום

מסמך מדיניות זה קובע את הקווים המנחים לפעילות אבטחת המידע של הארגון. אבטחת המידע היא לחם חוקו של הארגון, ואחד היסודות לאמון שניתן בו. מחויבות הנהלת הארגון, האמצעים המושקעים ביישום המדיניות, כמו גם הסנקציות שיוטלו על חריגה ממדיניות זו מעידים על מידת החשיבות הניתנת לנושא.

**על כלל עובדי הארגון ומנהליו, לפעול על פי מדיניות אבטחת מידע זו בכל היבטי פעולתם במסגרת הארגון.**

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

## נספח ח' - כתב מינוי ממונה אבטחת מידע

5/19/2021

ח' סיון תשפ"א

מינוי ממונה אבטחת מידע- עיריית הוד השרון

בהתאם לסעיף 17 ב' לחוק הגנת הפרטיות, התשמ"א- 1981 , הריני ממנה בזאת את אסף רבינוביץ, נושא ת.ז. 028409522 כממונה על אבטחת המידע במאגרים המוחזקים בעיריית הוד השרון.

תאריך: 19.05.2021

חתימה:

רן היילפרן
מנכ"ל
עיריית הוד השרון

## נספח ט' - הגדרת תפקיד ממונה אבטחת מידע

ממונה אבטחת מידע מונה באופן רשמי ב 19.5.2021,

תחום אחריותו:

- הכנת/ גיבוש נוהל אבטחת מידע ואישורו.
- הכנת תוכנית לביקורת שוטפת על העמידה בתקנות,
- ביצוע ביקורת בפועל, העברת הממצאים והמלצות וכו'

ממונה אבטחת מידע עובד בשוטף עם מנמ"רית העירייה ומנהל אבטחת מידע, אך ידווח לפרקים ועפ"י צורך למנכ"ל העירייה.

לממונה אבטחת המידע אצלנו יש עובד צמוד מטעמו המסייע לו בביצוע תפקידו,

אין לממונה אבטחת מידע כפיפים בעירייה.

תפקידים נוספים של ממונה אבטחת מידע: ייעוץ שוטף (טכנולוגי וארגוני).

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

## נספח י' - הצעת מחיר של איגוד אשכול השרון למנהל אבטחת מידע

16 אפריל 2020

לכבוד:

<u>גב' אילן כהן, מנמ"רית</u>

<u>עיריית הוד השרון</u>

שלום רב,

<u>הנדון: הצעת מחיר – מנהל אבטחת מידע עבור עיריית הוד השרון</u>

במסגרת ההסכם למתן שירותי מנמ"ריה בין עיריית הוד השרון לאשכול רשויות השרון, אשכול רשויות השרון מתכבד בזאת להגיש הצעת מחיר עבור שירותי מנהל אבטחת מידע לפי שעות.

השירות יינתן ע"י מנהל אבטחת מידע בעל תעודת CISO מורשה, ובעל ניסיון של מעל ל 10 שנים.

בהתאם לבחינת הצורך שנערכה, מדובר בכ-15 שעות שבועיות בממוצע.

השירות יכלול: ניהול ובקרה של מערך אבטחת המידע במועצה, בניית תוכנית עבודה שנתית ומעקב אחר ביצוע באופן שוטף, מילוי טפסים ובקשות בכל הקשור לאבטחת מידע וניהול מאגרי המידע מול משרד המשפטים, שליחת עדכונים לכלל עובדי המועצה בתחום אבטחת מידע, ביצוע בדיקות פתע וחדירות לתשתיות המחשוב.

התעריף המוצע (גלובלי) הינו 12,500 כולל מע"מ לחודש.

לכל מידע נוסף, הבהרות ניתן ליצור קשר מנמ"ר אשכול רשויות השרון.

בברכת המשך שיתוף פעולה פורה,

מוטי סרוסי

מנמ"ר אשכול רשויות השרון

העתק:

פז הירשמן - מנכ"ל אשכול רשויות השרון

## נספח י"א - מכרז לתפקיד מנהל / ת אבטחת מידע

**מכרז פומבי מס' 135/17 – לתפקיד מנהל/ת אבטחת מידע באגף מערכות מידע**

**תיאור התפקיד:**

**1. תכנון מדיניות אבטחת המידע ובקרה על יישומה**

א. שמירה ואבטחת המידע ברשות תוך דגש על אבטחת מידע רגיש ו/או מסווג והיבטים נוספים בהתאם להוראות הדין הקיים

ב. הגדרה ואשרור מדיניות אבטחת המידע ברשות בשיתוף מנהל מערכות המידע ותנהלת הרשות.

ג. יצירה ותחזוקה של רשימת מאגרי המידע העיקריים של כלל מערכות המידע והתקשורת בהתאם לדרישות החוק.

ד. סיווג נכסי המידע לפי רמת רגישותם והגדרת בקרות אבטחת המידע הנדרשות להם.

ה. הערכת סיכוני אבטחת המידע במערכת המידע והתקשורת.

ו. עדכון פרטי הערכת הסיכונים עם שינויים משמעותיים בתהליכים במערכות המידע או באיומי אבטחת מידע.

ז. רישום מאגרי מידע ועמידה בדרישות החוק בנושא אבטחת מידע והגנת הפרטיות.

ח. הגדרת דרישות אבטחת המידע ההכרחיות ליישום בתהליך העברת המידע ברשות ואל מחוץ לרשות המקומית.

ט. הגדרת אירועי אבטחת המידע וצורת התגובה לאירועים אלה.

י. הנחיית הנהלת הרשות המקומית בהפניית משאבים נאותים להטמעת אמצעי אבטחת מידע ולמיקוד בסקרי סיכוני אבטחת המידע במערכות המידע והתקשורת.

יא. הדרכת משתמשים בנושא אבטחת מידע.

יב. בקרה על יישום נוהלי אבטחת המידע ברשות.

יג. אחריות להחתמת עובדים חדשים ברשות המקומית בהתייחסות לאחריות העובד בכל הנוגע להיבטי אבטחת מידע שילווה בהצהרת סודיות.

יד. כתיבת נהלים לכל תהליך המטפל בניהול, הכנסה, תפעול, תחזוקה והוצאה של מידע ברשות המקומית בהתאם למדיניות וצרכי אבטחת המידע ברשות המקומית ויאשרם עם כתיבתם ו/או שינויים ויפעל להטמעתם.

**2. תכנון וביצוע סקרי אבטחת מידע**

א. ייזום סקרי אבטחת מידע של מערך מערכות המידע והתקשורת ברשות המקומית, עריכת סקרי אבטחת מידע לפני הטעמת שינויים משמעותיים או כאשר חלו שינויים במערכות המידע והתקשורת ברשות המקומית.

ב. בחינת יעילות אמצעי ההגנה שיושמו ברשות המקומית ורמת הגדרות אבטחת המידע במערכת המידע והתקשורת

ג. ייזום מבחני חדירה ( penetration tests) במערכות המידע והתקשורת להדמיית ניסיונות פריצה ע"י פורצים מתוך ומחוץ לרשות המקומית.

ד. הגדרת בקרות פיזיות, בהתאם להערכת הסיכונים, לאבטחת המידע. בקרות אלה יכללו נושאים כגון בקרת גישה, הגנה פיזית של נכסים וכו'

ה. וידוא כי סקרי אבטחת המידע ומבחני החדירה נערכים ע"י גורם מקצועי, עצמאי, בלתי תלוי וחיצוני לרשות המקומית.

**3. ניהול ההרשאות ודרכי הגישה למשתמשים**

א. חלוקת סביבת העבודה למעגלי אבטחה/ אזורים מאובטחים לפי רמות רגישות.

ב. יישום מנגנונים לניהול בקרות גישה במערכת מידע והתקשרות ברשות המקומית תוך מידור מתאים של הרשאות בין הרשות לגורמים חיצוניים.

ג. קביעת אמצעי זיהוי למערכות ושירותים לצורך זיהוי המשתמש תוך הקפדה על מניעת אפשרות העתקה או שחזור פריטי המידע של הרשות המקומית.

ד. הגדרת מדיניות סיסמאות ותהליכי גישה למערכות מידע והתקשרות ברשות המקומית.

**4. תכנון ויישום תכנית התאוששות- DRP**

א. פיתוח תוכנית התאוששות של מערכות המידע והתקשורת ממצבי חירום וממצבי משבר ברשות המקומית ( DRP - DISASTER RECOVERY PLAN)

ב. סיוע בקביעת תהליכים קריטיים שיש להפעיל במצבי משבר וחירום ברשות המקומית, בהתייחס למכלול היחידות של הרשות המקומית ובהתאם לצרכי הרשות.

ג. הקמת אתר חירום לצורך הפעלת מערך מערכות המידע והתקשורת לגיבוי מערך הנתונים, התומרה וכיו"ב ולהפעלתו מרגע התרחשות האסון, משבר או מצב חירום.

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

**5. ניהול ההגנה על מערכות המידע והתקשורת**

א. התקנת אמצעים המצמצמים את החשיפה לניסיונות פגיעה, כולל איתור, זיהוי ומניעה.
ב. הגדרת דרישות הגיבוי למערכות במידע והתקשורת ברשות המקומית בהתאם לצרכים השונים של הרשות המקומית.
ג. בקרת איכות הגיבויים ואופן אבטחתם.
ד. מתן אישור להעברת המידע בטרם העברת המידע לגוף ציבורי.

**ההעסקה מותנית בעמידה בנוהל איסור ניגוד עניינים**

**דרישות התפקיד:**

- ✓ בעל תעודת הנדסאי בתחום רלוונטי כדוגמת מתשבים /תוכנה /חומרה /מערכות מידע - חובה
- ✓ ניסיון מקצועי של 4 שנים לפחות כמנהל או כסגן מנהל מערכות מידע או מנהל אבטחת מידע בחברה בעלת 20 עובדים ומעלה - חובה.
- ✓ עברית ואנגלית ברמה גבוהה – חובה.
- ✓ העדר הרשעה בעבירה שבנסיבות העניין יש עמה קלון או בעברה מהעבירות המנויות בסעיפים 5 ו-31א לחוק הגנת הפרטיות (סעיף 17ב(ג)

**היקף המשרה**: מסלול קידום של מנהל מחלקה ברשות מקומית רמה ב' בדרוג הטכנאים וההנדסאים 39-41 או דרוג מח"ר בהתאם לכללים תנהוגים בשרות בציבורי או העסקה בחוזה אישי בכפוף לאישור משרד הפנים

**כפיפות**: מנהל מערכות מידע ראשי (מנמ"ר)

**כישורים אישיים:**
תפיסה אסטרטגית של מערכות המידע ברשות, יכולת עבודה בשיתוף פעולה עם כל יחידות הארגון, חדשנות, מציאת פתרונות טכנולוגיים בראיית עלות תועלת, יכולת חשיבה והפשטה לטווח ארוך, יכולת ארגון ותכנון, שקדנות, אמינות ומהימנות אישית, תפיסה שירותית גבוהה.

**מסמכים שיש לצרף לבקשה:**
קורות חיים
תעודות המעידות על השכלה וניסיון נדרשים
המלצות
צילום תעודת זהות
מועמד אשר יוזמן לועדת בחינה יידרש למלא הצהרה בדבר עברו הפלילי

מועמד העומד בתנאי המשרה והמעוניין בהגשת הצעה למשרה הנ"ל יגיש את הצעתו במעטפה סגורה ויפקידה בתיבת המכרזים באגף משאבי אנוש, בן גמלא 28, קומת ב',
עד **ליום א' 24/12/17 בשעה 13:00 (משרדי העירייה פתוחים כל יום עד השעה 15.30 וסגורים ביום שישי )**

מודגש בזאת כי העירייה שומרת על זכותה לבצע מיון מוקדם של ההצעות למשרה וכן הערכת המועמדים ע"י גורם מקצועי מטעם העירייה.

הצעות של מועמדים שתתקבלנה ללא הפרטים ו/או המסמכים כנדרש ו/או לאחר המועד הנקוב לעיל, לא תטופלנה ולא תובאנה לדיון בפני ועדת הבחינה.

**המשרה מיועדת לנשים וגברים כאחד.**

על החתום,

רינת סער פנקס
מנהלת אגף משאבי אנוש

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

**נספח י"ב - צו איגוד ערים (אשכול רשויות השרון) (תיקון) התשפ"א -2021**


רשומות

# קובץ התקנות

כ"ז בטבת התשפ"א | 9083 | 11 בינואר 2021


עמוד


כללי משק החשמל (אמות מידה לרמה, לטיב ולאיכות השירות שנותן ספק שירות חיוני) (תיקון מס' 7), התשפ"א–2021 ..... 1500

כללי משק החשמל (אמות מידה לרמה, לטיב ולאיכות השירות שנותן ספק שירות חיוני) (תיקון מס' 8), התשפ"א–2021 ..... 1503

כללי משק החשמל (אמות מידה לרמה, לטיב ולאיכות השירות שנותן ספק שירות חיוני) (הוראת שעה) (תיקון), התשפ"א–2021 ..... 1504

כללי משק החשמל (אמות מידה לרמה, לטיב ולאיכות השירות שנותן ספק שירות חיוני) (תיקון מס' 4) (תיקון), התשפ"א–2021 ..... 1504

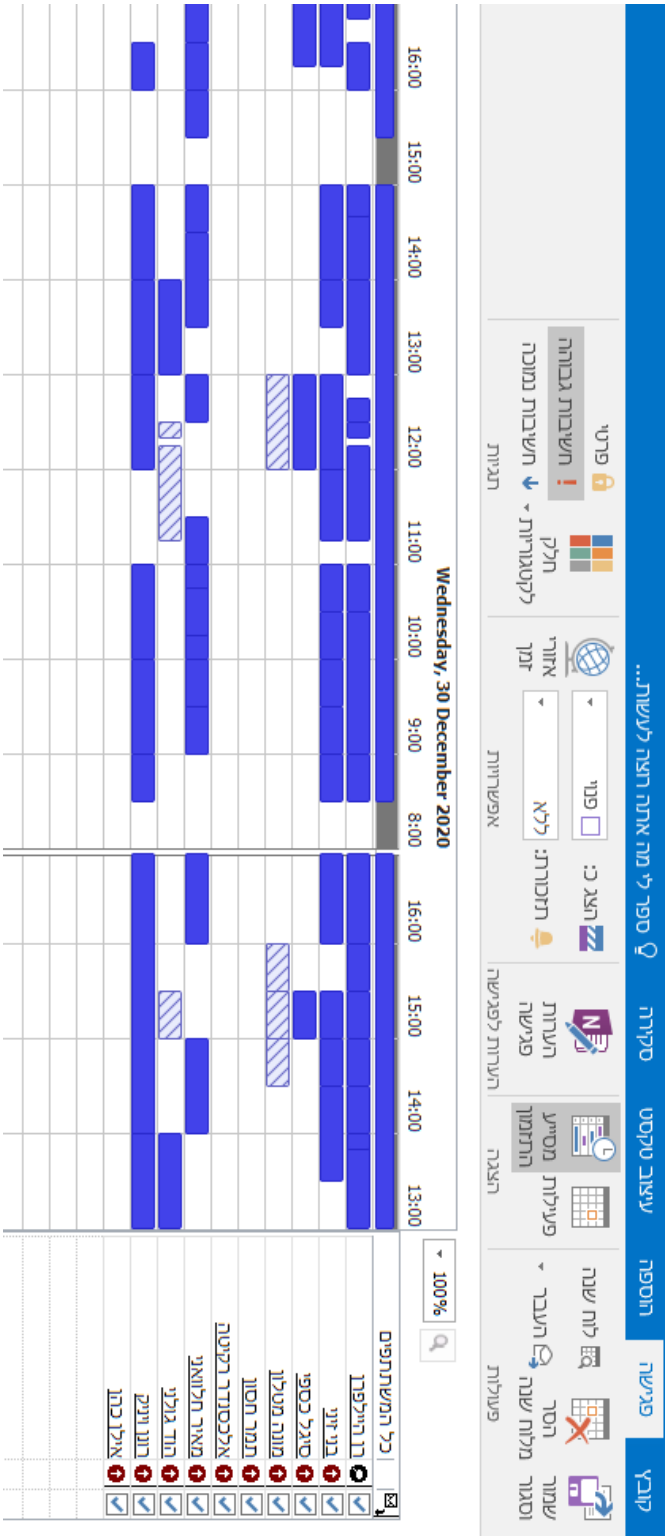
כללי משק החשמל (תעריפי חשמל) (תיקון מס' 5), התשפ"א–2021 ..... 1505

צו איגודי ערים (אשכול רשויות השרון) (תיקון), התשפ"א–2021 ..... 1506

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

## נספח י"ג - זימון לוועדת היגוי (לכאורה) לאבטחת מידע

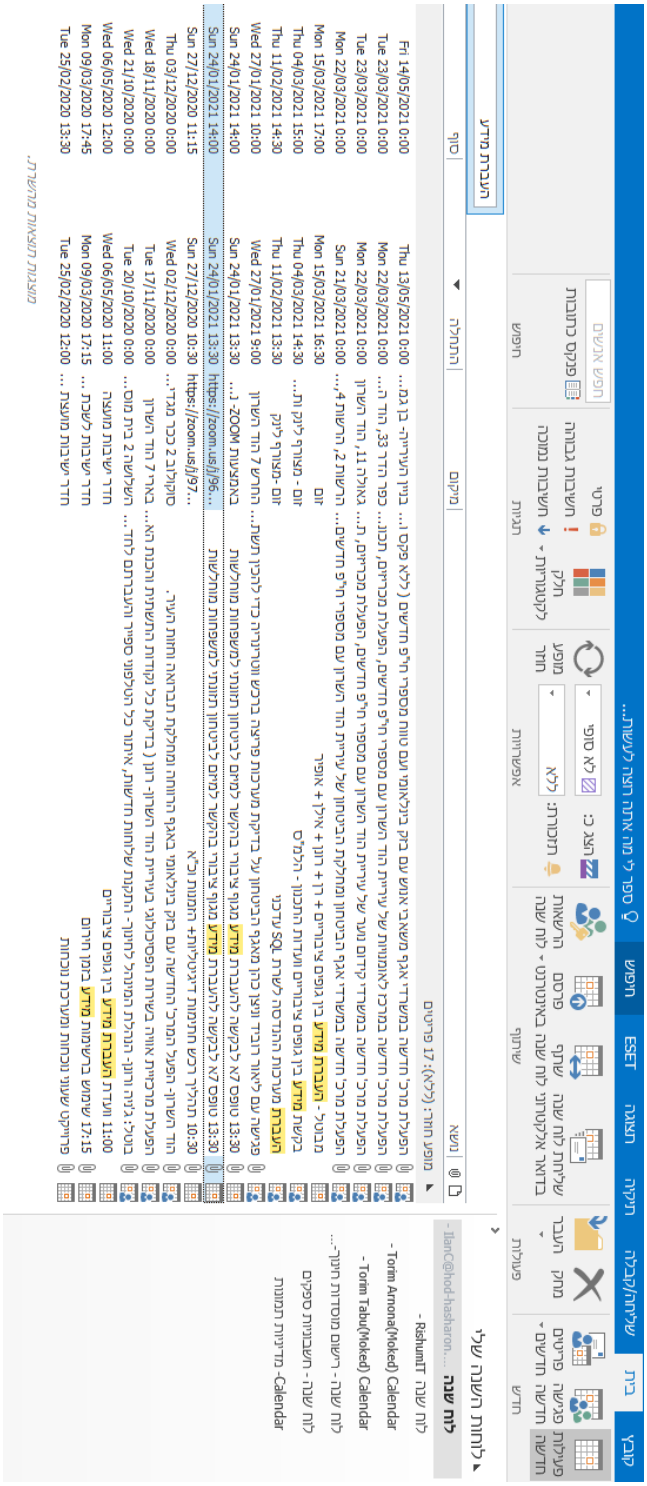
**זומנו לפגישות:**



**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

## נספח י"ד - זימון פגישות לעניין  אבטחת מידע (לכאורה)

### דוגמאות לפגישות:



**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

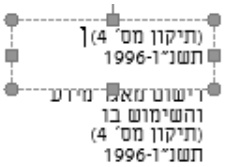
## נספח ט"ו - טבלת ריכוז מאגרי מידע שנתקבלה מאגף מערכות מידע

| # | אחסון | מספר מאגר 700067805 | | |

| # | אסמכתא | אישור משרד משפטים | כתב מינוי חתום | מאגר מידע | האם המאגר רשום | שם המאגר | מספר בני אדם כלולים במאגר | כמות משתמשים במאגר | מטרות המאגר | האם מידע מהמאגר מועבר לאחר? | רשימת מקבלי המידע מהמאגר | האם יש מחזיקים במאגר? | רשימת המחזיקים במאגר | רשום ברשות להגנת הפרטיות |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9 | 84910 | V | V | נתוני ספקים | לא | מערכת הנהלת חשבונות | 200,000 | מעל 101 | אספקת שרותים פיננסיים, | לא | | כן | מטרופולינט | מספר מאגר 700067834 |
| 10 | 84916 | V | V | נתוני עובדים | לא | מערכת שכר - מל"מ שכר | 100,000 | 11-30 | ניהול משאבי אנוש ושכר | לא | | כן | מל"מ שכר | מספר מאגר 700067835 |
| 11 | 84914 | V | V | נתוני עובדים | לא | מערכת נוכחות (PICO) | 100,000 | 11-30 | ניהול משאבי אנוש ושכר | כן | מל"מ שכר | לא | | מספר מאגר 700067839 |
| 12 | 84845 | | V | נתוני תושבים | לא | מערכת מוקד (CRMC) | 200,000 | 51-100 | דיווח ישיר וקשר עם הלקוח<br>מתן שירות ללקוחות<br>ניהול מידע על תושבים ומתן שירות לתושב | לא | | לא | | |
| 13 | 83949 | V | V | נתוני תושבים | לא | מערכת קומפלוט | 200,000 | 51-100 | ניהול מידע על תושבים ומתן שרות לתושב | לא | | לא | | |
| 14 | 84907 | V | V | נתוני נקנסים | לא | מערכת לנהול קנסות (COMAX) | 2,000,000 | 51-100 | ניהול מידע על תושבים ומתן שרות לתושב | כן | לינט גבייה | כן | מילאון | מספר מאגר 700067833 |
| 15 | 83917 | V | V | תמונות שטח/ | לא | מערך מצלמות | 100,000 | עד 10 | ביצוע תפקידים על פי דין אחר רגיש | לא | | לא | | |
| 16 | לא נדרש | | | wiseinfo | לא | מערכת לרישום חוגים | 100,000 | עד 10 | שמירת דיווחים של הצהרת בריאות קורונה לפי נוהלי משרד הבריאות | לא | | כן | wiseinfo | |
| 17 | 84639 | V | V | אתר עירוני | | אתר אינטרנט רשותי | 100,000 | עד 10 | אספקת שרותים לתושבים | לא | | כן | א.ש בינה | |
| 18 | 84922 | V | V | סנסורי | לא | ניהול סייעות חינוך AssisNet | 100,000 | עד 10 | ניהול משאבי אנוש ושכר | כן | שכר, פיקו | כן | סנסורי | מספר מאגר 700067821 |
| 19 | 83925 | V | V | מערכת לומדות | לא | מאגר לומדות לעובדי הארגון | 100,000 | עד 10 | ניהול משאבי אנוש, מבדקים לעובדים | לא | | כן | I'm Learning | |
| 20 | 84870 | V | V | וטקליק | | ניהול מחלקה וטרינרית וטקליק | | | | | | | | מספר מאגר 700067826 |
| 21 | ללא | | | תמונות עובדים | | | | | | | | | | |

לשכת מבקר העירייה
והממונה על תלונות הציבור

## נספח ט"ז - רישום מאגר מידע עפ"י חוק הגנת הפרטיות


[תיקון מס' 4]
תשנ"ו-1996
רישום מאגר מידע והשימוש בו
(תיקון מס' 4)
תשנ"ו-1996

סימן א': מאגרי מידע

8. (א) לא ינהל אדם ולא יחזיק מאגר מידע החייב ברישום לפי סעיף זה, אלא אם כן התקיים אחד מאלה:

(1) המאגר נרשם בפנקס;

(2) הוגשה בקשה לרישום המאגר והתקיימו הוראות סעיף 10(ב1);

(3) המאגר חייב ברישום לפי סעיף קטן (ה) והוראת הרשם כללה הרשאה לניהול והחזקה של המאגר עד רישומו.

(ב) לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר.

(ג) בעל מאגר מידע חייב ברישום בפנקס ועל בעל המאגר לרשמו אם נתקיים בו אחד מאלה:

(1) מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000;

(2) יש במאגר מידע רגיש;

(3) המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמם או בהסכמתם למאגר זה;

(4) המאגר הוא של גוף ציבורי כהגדרתו בסעיף 23;

(5) המאגר משמש לשירותי דיוור ישיר כאמור בסעיף 17ג.

(ד) הוראת סעיף קטן (ג) לא תחול על מאגר שאין בו אלא מידע שפורסם לרבים על פי סמכות כדין או שהועמד לעיון הרבים על-פי סמכות כדין.

(ה) הרשם רשאי, מטעמים מיוחדים שיירשמו, להורות על קיום חובת רישום לגבי מאגר הפטור מחובת רישום לפי סעיפים קטנים (ג) ו-(ד); הוראה כאמור תומצא לבעל המאגר ובה יפרט

(תיקון מס' 7)
תשס"ה-2005



נבו הוצאה לאור בע"מ nevo.co.il המאגר המשפטי הישראלי

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

חוק הגנת הפרטיות, תשמ"א-1981
נוסח מלא ומעודכן

הרשם הוראות לענין ניהול ואחזקת המאגר עד לרישומו.

בקשה לרישום

9. (א) בקשה לרישום מאגר מידע תוגש לרשם.

(תיקון מס' 4) תשנ"ו-1996

(ב) בקשה לרישום מאגר מידע תפרט את –

(1) זהות בעל מאגר המידע, המחזיק במאגר ומנהל המאגר, ומעניהם בישראל;

(2) מטרות הקמת מאגר המידע והמטרות שלהן נועד המידע;

(3) סוגי המידע שייכללו במאגר;

(4) פרטים בדבר העברת מידע מחוץ לגבולות המדינה;

(5) פרטים בדבר קבלת מידע, דרך קבע, מגוף ציבורי כהגדרתו בסעיף 23, שם הגוף הציבורי מוסר המידע ומהות המידע הנמסר, למעט פרטים הנמסרים בהסכמת מי שהמידע על אודותיו.

(תיקון מס' 5) תש"ס-2000

(ג) שר המשפטים רשאי לקבוע בתקנות פרטים נוספים שיפורטו בבקשה לרישום.

(ד) הבעל או המחזיק של מאגר מידע יודיע לרשם על כל שינוי בפרט מהפרטים המפורטים בסעיף קטן (ב) או לפי סעיף קטן (ג) ועל הפסקת פעולתו של מאגר המידע.

סמכויות הרשם (תיקון מס' 4) תשנ"ו-1996

10. (א) הוגשה בקשה לרישום מאגר מידע –

(1) ירשום אותו הרשם בפנקס, תוך 90 ימים מיום שהוגשה לו הבקשה, זולת אם היה לו יסוד סביר להניח כי המאגר משמש או עלול לשמש לפעולות בלתי חוקיות או כמסווה להן, או שהמידע הכלול בו נתקבל, נצבר או נאסף בניגוד לחוק זה או בניגוד להוראות כל דין;

**נספח י"ז – המאגרים שנרשמו בפנקס מאגרי המידע במשרד המשפטים**

| | | | |
|---|---|---|---|
| FW מ -700067805 'מס מאגר רישום מאישור... | 01/06/2021 12:16 | CoolUtils Mail Vie... | 1,676 KB |
| FW מ -700067810 'מס מאגר רישום מאישור... | 01/06/2021 12:16 | CoolUtils Mail Vie... | 1,794 KB |
| FW סנ -700067821 'מס מאגר רישום מאישור... | 01/06/2021 12:16 | CoolUtils Mail Vie... | 1,631 KB |
| FW מ -700067826 'מס מאגר רישום מאישור... | 01/06/2021 12:16 | CoolUtils Mail Vie... | 1,632 KB |
| FW מ -700067833 'מס מאגר רישום מאישור... | 01/06/2021 12:16 | CoolUtils Mail Vie... | 1,653 KB |
| FW מ -700067834 'מס מאגר רישום מאישור... | 01/06/2021 12:16 | CoolUtils Mail Vie... | 1,632 KB |
| FW מ -700067835 'מס מאגר רישום מאישור... | 01/06/2021 12:16 | CoolUtils Mail Vie... | 1,631 KB |
| FW סנ -700067836 'מס מאגר רישום מאישור... | 01/06/2021 12:16 | CoolUtils Mail Vie... | 1,631 KB |
| FW מ -700067839 'מס מאגר רישום מאישור... | 01/06/2021 12:16 | CoolUtils Mail Vie... | 1,630 KB |

## נספח י"ח - דוגמאות לרישום מאגרי מידע בפנקס המאגרים – משרד המשפטים

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

תאריך: אי סיון תשפ"א
12 במאי 2021
סימוכין: 008-2021-00008971
מזהה אינטרנט: DDB0963A83
באמצעות: דוא"ל

לכבוד
עירית הוד השרון
הוד השרון

א.ג.נ,

הנדון: **אישור על רישום מאגר מידע בפנקס מאגרי המידע**
**מס' מאגר**: 700067805 **שם המאגר**: מערכת מטרופולינט- גבייה, חינוך, חוגים
**בבעלות** עירית הוד השרון **מס' זיהוי**: 500297007

מתוקף סמכותי לפי חוק הגנת הפרטיות, התשמ"א – 1981 (להלן - **החוק**), ובהתאם להוראותיו, המאגר שבנדון נרשם בפנקס מאגרי המידע בהתאם לפרטים שנמסרו בבקשת הרישום ובכפוף לתנאים כלהלן:

1. איסוף המידע מנושא המידע - הפרט אשר מידע אודותיו מעובד, ייעשה תוך מתן **הודעה מפורשת**, כאמור בסעיף 11 לחוק.
2. ההודעה לפי סעיף 11 לחוק תינתן באחד מהאופנים הבאים:
   - טופס הסכמה מודפס
   - טופס הסכמה מקוון
   - דוא"ל
   - שיחה בעל פה מתועדת
3. הודעה וההסכמה צריכות להינתן למבקש המידע באופן ישיר ואין להסתמך על הסכמות שניתנו לצדדי ג' אלא אם בהודעה שניתנה על ידיהם צוין במפורש שהמידע יועבר לבעל המאגר שלעיל.
4. בהתאם לבקשת הרישום, מנהל המאגר המוסמך לביצוע תפקידיו לפי החוק והתקנות הוא: זיני בני.
5. כבעל המאגר הצהרת, כי המידע נאסף למאגר למטרת דיוור ישיר וקשר עם הלקוח ונעשה בו שימוש לפי הוראות החוק.
6. תשומת לבך מופנית לעובדה, כי חל איסור לסטות ו/או לעשות שימוש אחר, מכל סוג שהוא, לרבות העברת מידע, בעקיפין או במישרין, מהמטרה המפורטת לעיל ומיתר הפרטים שמולאו בבקשה, וזאת כדי למנוע מעשה המהווה הפרת חובה חוקית, על כל מה שמשתמע ומתחייב מכך, הפעלת סמכויות רשם מאגרי המידע ונקיטת סנקציות משפטיות לפי חוק הגנת הפרטיות, התשמ"א – 1981.



073-3928555 | 02-6467064 | PPA@justice.gov.il
קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | WWW.PPA.JUSTICE.GOV.IL

7. נכונות ואמיתות המידע שנמסר בבקשת רישום המאגר / בקשת עדכון הפרטים / המענים לדרישת קבלת המסמכים, מהווים תנאי לתוקפו של אישור זה.

בכבוד רב,

צחי פנחס

מ"מ רשם מאגרי המידע

הרשות להגנת הפרטיות

***האמור מעלה מעיד על הרישום בפנקס המבוסס על הצהרות בעל המאגר כאמור לעיל.***
***מצ"ב העתק כרטיס המאגר מפנקס המאגרים ובו פרטי המאגר. בכל הצגה של כרטיס המאגר חובה להציג גם מכתב זה.***
***אין ברישום כדי לאשר כי המידע נאסף למאגר ונעשה בו שימוש בהתאם להוראות החוק. בעל המאגר ומנהל המאגר מופנים להוראות החוק התקנות והנחיות הרשם המפורסמות באתר הרשות להגנת הפרטיות כדי לעמוד על חובותיהם המפורטות בחוק.***
***להבהרות או שאלות בדבר התאמה של הפעילות להוראות החוק ניתן לפנות אל הרשם לפי נוהל בקשה לפנייה מוקדמת.***



PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | קרית הממשלה, ת.ד. 7360, תל אביב 6107202

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

תאריך: אי סיון תשפ"א
12 במאי 2021
סימוכין: 008-2021-00008954
באמצעות: דוא"ל

לכבוד
עיריית הוד השרון
הוד השרון

א.ג.נ,

הנדון: **אישור על רישום מאגר מידע בפנקס מאגרי המידע**
**מס' מאגר**: 700067821 **שם המאגר**: סנסורי ניהול סייעות חינוך
**בבעלות** עיריית הוד השרון **מס' זיהוי**: 500297007

בהתאם לסעיף 8 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן - **החוק**) הריני לאשר כדלקמן:

1. המאגר שבנדון נרשם בפנקס מאגרי המידע בהתאם לפרטים שנמסרו בבקשת הרישום.
2. בהתאם לבקשת הרישום הצהיר בעל המאגר כי המידע נאסף למאגר ונעשה בו שימוש בהתאם להוראות החוק.
3. בהתאם לבקשת הרישום מנהל המאגר המוסמך לביצוע תפקידיו לפי החוק והתקנות הוא: **אפרתי מיכל**.

בכבוד רב,

צחי פנחס
מ"מ רשם מאגרי המידע
הרשות להגנת הפרטיות

***האמור מעלה מעיד על הרישום בפנקס המבוסס על הצהרות בעל המאגר כאמור לעיל.***
***מצ"ב העתק כרטיס המאגר מפנקס המאגרים ובו פרטי המאגר. בכל הצגה של כרטיס המאגר חובה להציג גם מכתב זה.***
***אין ברישום כדי לאשר כי המידע נאסף למאגר ונעשה בו שימוש בהתאם להוראות החוק. בעל המאגר ומנהל המאגר מופנים להוראות החוק התקנות והנחיות הרשם המפורסמות באתר הרשות להגנת הפרטיות כדי לעמוד על חובותיהם המפורטות בחוק.***
***להבהרות או שאלות בדבר התאמה של הפעילות להוראות החוק ניתן לפנות אל הרשם לפי נוהל בקשה לפנייה מוקדמת.***



PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | קריית הממשלה, ת.ד. 7360, תל אביב 6107202

**נספח י"ט - מאגרי מידע שחלה עליהם רמת אבטחה בינונית וגבוהה**

תוספת ראשונה

(תקנה 1 והתוספת השנייה)

1. מאגרי מידע שחלה עליהם רמת האבטחה הבינונית– (1) מאגר מידע שמטרתו העיקרית היא איסוף מידע לצורך מסירתו לאחר כדרך עיסוק ,לרבות שירותי דיוור ישיר;

(2) מאגר מידע שבעליו הוא גוף ציבורי כמשמעותו בסעיף 23 לחוק ,אף אם לא התקיימו בו הוראות פסקה (1) או (3).

(3) מאגר מידע הכולל מידע שהוא אחד מאלה:

(א ) מידע על צנעת חייו האישיים של אדם ,לרבות התנהגותו ברשות היחיד;

(ב ) מידע רפואי או מידע על מצבו הנפשי של אדם;

(ג ) מידע גנטי כהגדרתו בחוק מידע גנטי ,התשס"א- 2000;

(ד ) מידע על אודות דעותיו הפוליטיות או אמונותיו הדתיות של אדם;

(ה ) מידע על אודות עברו הפלילי של אדם;

(ו ) נתוני תקשורת כהגדרתם בחוק סדר הדין הפלילי( סמכויות אכיפה- נתוני תקשורת ,)התשס"ח- 2007;

(ז ) מידע ביומטרי;

(ח ) מידע על נכסיו של אדם ,חובותיו והתחייבויותיו הכלכליות ,מצבו הכלכלי או שינוי בו ,יכולתו לעמוד בהתחייבויותיו הכלכלית ומידת עמידתו בהם;

(ט ) הרגלי צריכה של אדם שיש בהם כדי ללמד על מידע לפי פרטים (א) עד (ז) או על אישיותו של אדם , אמונתו או דעותיו.

2. על אף האמור בפרט 1 (3) על מאגר מידע המקיים אחד מאלה ,לא חלה רמת האבטחה הבינונית אלא רמת האבטחה הבסיסית:

(1) המאגר כולל מידע מן הסוגים המפורטים בפרט 1 (3) (ב) , (ה), (ו), (ז) לעניין תמונות פנים בלבד ו - (ח) , על אודות המועסקים או הספקים של בעל מאגר המידע,

ובלבד שהמידע משמש למטרות ניהול העסק בלבד ,ואינו כולל מידע מן הסוגים המפורטים בפרט 1 (3) (א), (ג), (ד) ו- (ז) לעניין מידע שאינו תמונות פנים ו- ( ט) .

(2) מספר בעלי ההרשאה אצל בעל המאגר אינו עולה על עשרה.

ביטול

4

**תוספת שנייה**

**(תקנה)1**

מאגרי מידע שחלה עליהם רמת האבטחה הגבוהה-

(1) מאגר מידע כאמור בפרט 1 (1) או (3) בתוספת הראשונה ,לרבות מאגר של גוף ציבורי

כמשמעותו בסעיף 23 (1) לחוק המקיים את האמור בפרטים (1) או (3) שיש בו מידע על אודות 100,000 אנשים ומעלה;

(2) מאגר מידע כאמור בפרט 1 (1) או ( 3 ) בתוספת הראשונה ,לרבות מאגר של גוף ציבורי

כמשמעותו בסעיף 23 (1) לחוק המקיים את האמור בפרטים (1) או (3) שמספר בעלי ההרשאה בו עולה על. 100

לשכת מבקר העירייה
והממונה על תלונות הציבור

נספח כ'

## סקר אבטחת מידע 2018

תוכנית ליישום

מה תאריך התוכנית? זאב (04/07/21)

| מס' | ממצא | פעולה | אחריות | סטטוס/הערות |
|---|---|---|---|---|
| 1 | פעיל בין "קומפלוט" ל"עירייה" עם הרשאות מלאות בארגון S2S | לבטל VPN S2S | אלכס | |
| | | לאשר VPN אך ורק על פי צורך ועל ידי FA 2 | ולד/אלכס | בתהליך קבלת הצעת מחיר לביצוע |
| | | לנהל נוהל עבודה עם ספקים ולהחתים ספקים על סקר אבטחת מידע | אלכס | |
| 2 | סיגמנטציה | הפרדה מלאה של סביבת השרתים וסביבת המשתמשים | אלכס | |
| | | לבחון כל פורט או פרוטוקול אשר עובד בין הסביבות | אלכס | |
| | | להוציא שרתים אשר מתחברים לאינטרנט ל DMZ נפרד | אלכס | |
| 3 | הצפנת מידע | הנחייה לעובדים שמירת מידע על גבי שרתי העירייה בלבד | ולד | |
| | | הצפנת מידע במחשבים ניידים ו או מחשבים רגישים בעירייה | ולד | המלצה להטמיע BITLOCKER |
| | | לבצע גיבוי ברמה יומית | ולד | מבקש לקבל דוח חודשי לגיבויים + מדיניות גיבויים |
| 4 | ניהול F.W | בדיקת חוקים | אלכס | קבלת דוח פירוט חוקים מוגדרים, הגדרת חוקים חדשים מחייב אישור עפ"י נוהל שנשלח |

לשכת מבקר העירייה
והמועצה על תלונות הציבור

| מס' | ממצא | פעולה | אחריות | סטטוס/הערות |
|---|---|---|---|---|
| 5 | כלל העובדים בעלי הרשאות ניהול מקומי על המחשבים | נדרש כי הרשאות המשתמשים ברשת יהיו במינימום הנדרש לצורך ביצוע עבודתם. | ולד | |
| | | נדרש כי הרשאותת ניהול יהיו מוגבלות לצוות IT בלבד , חריגות יבחנו בקפידה ובמידת האפשר יהיו תחת ניטור. | ולד | |
| | | בכל מקרה, משתמשים בעלי הרשאות ניהול לא יבצעו התחברות לרשתבאמצעות הרשאות אלה, ההתחברות תתבצע באמצעות משתמש "פשוט" Run as Administrator". ובעת הצורך יעשה | ולד | |
| 6 | שרתים ועמדות – חוסר עדכוני אבטחה | להגדיר נוהל עדכונים מסודר | ולד | הפצת דוח סטטוס חודשי, ביצוע הפצה באופן מידי |
| 7 | ניהול הרשאות – הפרדת סמכויות ADMIN | לייצר שני משתמשים שונים, האחד לללניהול המערכת והשני לעבודה השוטפת | ולד | ליישם במידי |

לשכת מבקר העירייה
והממונה על תלונות הציבור

| מס' | ממצא | פעולה | אחריות | סטטוס/הערות |
|---|---|---|---|---|
| 8 | הקשחת שרתים ועמדות קצה אינה אופטימלי | מתודולגיית הקשחה לשרתים והמחשבים | ולד | שדרוג מערכות ישנות, הטמעת best practice |
| | | חסימת USB | ולד | מבוצע , להוסיף התקנים נוספים במידת הצורך |
| 9 | מדיניות ניהול סיסמאות של "העירייה" | סיסמא מורכבת, החלפה כל 3 חודשים | ולד | על פי הנוהל שנשלח |
| 10 | תכנית DRP | כתיבת תוכנית DRP | אסף/אלכס/ולד | כולל תקשורת ושרתים, ניתן ליישם גם באמצעות העלאת שרתי העירייה לענן |
| 11 | העדר מערכת לזיהוי אנומליות ברשת | ממולץ להטמיע צערכת כדוגמת PROMISEC | אלכס | בודק הטמעה דרך בזק |
| 12 | אין הוצאות גיבויים מחוץ למתחמי "העירייה" | להטמיע במסגרת נוהל הגיבויים | ולד | ניתן לבחון גיבוי לענן AZURE או לבחון העלאת כלל השרתים לאירוח בענן |
| 13 | מערכת ניהול לוגים ואירועים SIEM | הטמעת מערכת בשירות ענן | אסף/אלכס/ולד | הועברה הצעת מחיר לביצוע |
| 14 | היעדר בקרה על חיבור פיזי לרשת הארגון | הטמעת מערכת NAC | ולד/אלכס/אסף | קבלת הצעות מחיר |
| 15 | העדר מנגנון ארגוני לניהול אבטחת מידע | הטמעת נוהל אבטחת מידע | אסף/אלכס/ולד | הועבר נוהל בנושא |

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

**נספח כ"א**

**דו"ח סיכום אבטחת מידע ומאגרי מידע לפתרון - יוני 2021**

| תאריך | תאור | סוג פגיעה | המלצות | |
|---|---|---|---|---|
| 25.04.2021 | מדע ל שקראות מאזעקות לא רגיעו למערכת המרכזית במשך 3 ימים | 3 ימים כל המערכות אזעקה לא תפקדו כולל מערכת של חדרי השרתים, כולל חיישני טמפרטורה,וכו' | 1. לבדוק תקינות של המערכת<br>2. להסדיר עבודה מול ספקי שירות.<br>3. להקפיד על ביצוע נוהלים במוקד העירוני | |
| 26.04.2021 | מדע ל שטרם סגורה אפשרות עברת קבצים דרך USB | 1. דליפת מידע<br>2. הפצת וירוסים | 1. לחזק פוליסי . | |
| 29.04.2021 | ממחשב PC במח' התחדשות הערנית הפעיל WIFI והתחבר לרשת FREE | חיבור בו זמני לך רשתות | 1. לבדוק ביטול כרטיסי WIFI בכל המחשבים המחוברים לרשת LAN .<br>2. לחזק את החוקים ע"מ לא לתת אפשרות להפעיל את הכרטיס WIFI | **טופל** |
| 02.05.2021 | תמונת עובדים אשר צלמו לבשביל כרטיסי נוכחות השבה מעבר לעירייה ללא הסכמת עובדים ולמטרת לא ברורות | דליפת מידע רגיש (אישי) שימוש במידע למטרות אחרות | 1. להגדיר מטרת ברורות בשימוש במידע אישי<br>2. לבצע עברות מידע באופן מסודר<br>3. לבמת מנהל שמסדיר פעולות כאלו. | |
| 06.05.2021 | השבונות אנשים אשר עזבו את העירייה פעילים ופתוחים | גישת משתמשים לא מורשים | 1.לבצע סגירת חשבונות.<br>2. להקפיד על ביצוע נוהל עזיבת עובד | |
| 23.05.2021 | מדע ל שמשתמשת תדשה שיר טמסיט זמן רב התמשה בחשבון מחשב של מרית גרטב באגף הרווחה | גישת משתמשים לא מורשים | 1. להסביר ביח' הרלאוונטיות (משאבי אנוש, חוחה) על נוהלים<br>2. להקפיד על ביצוע נוהלים | |
| 30.05.2021 | שולחן עבודה במחשב של קב"סית ניצה מכל קבצים מסוג סוד ביותר (מידע רפואי) | חשיפת מידע מסווג | 1. להסביר למשתמשים חשיבות .<br>2. לדרוש ממנהלים להקפיד על ביצוע נוהל עבודה ואבטחת מידע | |

**נספח כ"ב**

סימוכין:222920

נוהל מס' 1.00.01

## אבטחת מידע בשימוש במכשירים ניידים

הנוהל מתייחס לשימוש במכשירים ניידים אשר מחוברים למערכת הדוא"ל הארגוני (EXCHANGE)

מכשיר נייד - סמארטפון, טבלאט או כל מכשיר נייד אחר אשר מחובר למערכת הדוא"ל הארגונית באופן קבוע.

משתמש – אדם החתום בטופס ההתחייבות

סלולארי ( אין תלות בבעלות המכשיר ו/או מנוי SIM)

אין תלות באופן חיבור – סלולארי בלבד, סלולארי + WIFI, WIFI בלבד או כל חיבור אחר

אין תלות בסוג המכשיר, יצרן או מערכת הפעלה ANDROID, MICROSOFT, APPLE וכו'

אין תלות בסוג התיקיות המסונכרנות – דואר לו"ז בלד, וכו'

הנוהל קובע את סדר הפעולות אשר מתבצעות ברגע שהמכשיר **לא נמצא** בידי המשתמש.

## נוהל

כאשר המכשיר הנייד לא נמצא בידי המשתמש (נגנב, נמסר לתיקון, אבד או כל סיבה אחרת)

**באחריות המשתמש** להודע למנהל הרשת באופן מיידי בכל דרך אפשרית 24 שעות, 7 ימים.

במקרה של מסירת מכשיר לידי אדם אחר באופן יזום (מסירה לתיקון, העברה בין בני משפחה,

או בכל מקרה אחר) **באחריות המשתמש** להודיע לפני המסירה.

במקרה של אי עמידה בנוהל הזה המכשיר ינותק ממערכת הEXCHANGE

באחריות המשתמש להכיר את כל השינויים בנוהל זה.

אני החתום מטה: _____ ת.ז _____

**קראתי את הנוהל ותחייב לפעול על פיו**

חתימה _____ תאריך _____

## נספח כ"ג - הרשת הפנימית הגנה על גישה למאגרי מידע

(1) כיום קיימת הגנה לגישה למאגרי מידע:
גישה למאגרי מידע פנימיים מוגנת ע"י מערכת חומת אש (FW ) ומערך הרשאות.

(2) חלק מעמדות העבודה מבודדות ע"י סגמנטציה בציוד התקשורת

(3) הסגמנטציה מתבצעת ברמה של מחלקות .

(4) כ"כ קיימים סגמנטים נפרדים של ציודים ברשת :

- מדפסות
- מתגי מחשוב
- מתגי טלפוניה
- טלפונים IP
- שעוני נוכחות
- ציוד נלווה (קיוסקים)

(5) כ"כ עמדות אשר נמצאות בסניפים מרוחקים מבודדות מעמדות עבודה של אותה מחלקה הנמצאות בסניף אחר או בבניין העירייה (אגף הרווחה לדוגמה)

## נספח כ"ד - אבטחת תקשורת - חיבורים לרשת

1. חיבורים לרשת האינטרנט ורשתות של ספקים אחרים מוגנים ע"י מערכת חומת אש (FW)
2. גלישה ברשת האינטרנט מתבצעת ע"י מערכת PROXY . מגבלות גלישה הנן לפי תפקיד
3. כניסה לLAN מתבצע ע"י חיבור SSL VPN או ע"י מערכות שליטה מרחוק של העירייה וספקים
4. אין כניסה חופשית על תוך הLAN.

## נספח כ"ה - ההסכם עם חברת מטריקס - עמוד ראשון

42/19

**מכרז מס' מח/6/2018**

**חוזה התקשרות**

שנערך ונחתם ב_____

ביום 5 לחודש 3 לשנת 19

**בין:**

**עיריית הוד השרון**

**(להלן: "הרשות המזמינה")**

**לבין:**

מטריקס אי.טי. אינטרגרציה

**מס' תאגיד רשום 511204026**

**(להלן: "הספק")**

**והואיל** והספק הינו אחד הזוכים במכרז מס' מח/6/2018 לשירותי IT - סייבר, אחסון, ציוד היקפי ושירות שפורסם על ידי החברה למשק וכלכלה של השלטון המקומי בע"מ (להלן: "**המכרז**");

**והואיל** וברצון הרשות המזמינה להזמין מהספק שירותי אספקה, התקנה ותחזוקה של מחשבים וציוד היקפי בהתאם לתנאי המכרז, בנוהל הצעת מחיר מס' B-402108-18-13836, והספק מעוניין ליתן לרשות המזמינה שירותים, כאמור, והכול בתנאים המפורטים במסמכי המכרז;

**לפיכך הוצהר, הוסכם והותנה בין הצדדים כדלקמן:**

1. הרשות המזמינה מזמינה בזאת מהספק את ביצוע השירותים המפורטים בחוזה זה, על פי מסמכי המכרז ותנאי ההתקשרות הרצ"ב כחלק בלתי נפרד מחוזה זה (להלן: "**השירותים**").

2. הספק מתחייב לספק לרשות המזמינה את השירותים, בהתאם למפורט בחוזה זה ועל פי מסמכי ותנאי המכרז.

3. <u>חלופה ב'</u>

בגין שירותי תחזוקה של מחשבים וציוד היקפי / שירותי טכנאים / של מערכות אחסון ואבטחת מידע, אשר הוזמנו מהספק, כמפורט <u>בנספח ב'</u> לחוזה זה – סכום החוזה הינו 142,078 ₪ לחודש (לא כולל מע"מ), ובסה"כ 5,114,808₪ (לא כולל מע"מ) לכל תקופת ההתקשרות של שלושים ושישה (36) חודשים, הכל בהתאם להצעת הספק בנוהל הצעת הטחירים.

מטריקס אי.טי
אינטגרציה (1998) בע"מ

עיריית הוד השרון
THE MUNICIPALITY OF HOD HASHARON

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

## נספח כ"ו

## תצהירי ונספחי אבטחת מידע לחתימת ספקי האגף

**אגף מערכות מידע**

**טלפון: 09-8894070**

4/30/2021

לח' איר תשפ"א

לכבוד

חב' מלם שכר

המחזיק מאגר מידע של עיריית הוד-השרון: מערכת שכר, מס' _____

א.נ.,

**הנדון: תצהיר אבטחת מידע**

בהתאם להוראות התקנות, מחזיק מאגר מידע נדרש לדווח לרשות, אחת לשנה לפחות, אודות אופן ביצוע חובותיו לפי תקנות אבטחת המידע. על כן, נודה לקבלת תגובתכם האם הנכם עומדים בהוראות תקנות אבטחת המידע המפורטות במכתב זה ובאיזה אופן

אבקשכם למלא את השאלון ולהעביר חתום למנהל אבטחת מידע :

**אלכס רקיטה, rakita@hod-hasharon.muni.il , 0505235704**

1. האם מצהיר כי הוא פועל כנדרש על פי החוק, התקנות ותיקוני הצנת הפרטיות וכי הוא מקט באמצעי אבטחה ובקרה כמתחייב מהוראות חוק הגנת הפרטיות, תיקוניו ותקנותיו והנחיות רשם מאגרי מידע

כן לא.

2. האם מונה באירגון אחראי לאבטחת מידע ?

לא

כן :

שם פרטי_____, שם משפחה_____, תפקיד_____

טל'_____, E-Mail_____

3. האם קיימים נוהלי אבטחת מידע באירגון ?

כן לא

4. האם קיים מסמך מעודכן של מבנה המאגר כמפורט בתקנה 5 לתקנות אבטחת המידע ?

כן לא

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

**אגף מערכות מידע**

**טלפון: 09-8894070**

4/30/2021

ל"ח אייר תשפ"א

לכבוד

חב' **סנסורי פתרונות תוכנה בע"מ**

המחלק מאגר מידע של עיריית הוד-השרון: **מערכת לניהול סייעות חיצוני**, מס' _____

א.ג.נ

**הנדון: תצהיר אבטחת מידע**

בהתאם להוראות התקנות, מחזיק מאגר מידע נדרש לדווח לרשות, אחת לשנה לפחות, אודות אופן ביצוע חובותיו לפי תקנות אבטחת המידע. על כן, נודה לקבלת תגובתכם האם הנכם עומדים בהוראות תקנות אבטחת המידע המפורטות במכתב זה ובאיזה אופן

אבקשכם למלא את השאלון ולהעביר חתום למנהל אבטחת מידע :

**אלכס רקישה, rakita@hod-hasharon.muni.il , 0505235704**

1. המפקח מצהיר כי הוא פועל כנדרש על פי החוק, התקנות ותיקוני הגנת הפרטיות וכי הוא מקפיד באמצעי אבטחה ובקרה כמתחייב מהוראות חוק הגנת הפרטיות, תיקוניו ותקנותיו והנחיות רשם מאגרי מידע

   כן  לא

2. האם מונה בארגונך אחראי לאבטחת מידע ?

   לא

   כן :

   שם פרטי_____, שם משפחה_____, תפקיד_____

   טל_____, E-Mail_____

3. האם קיימים נוהלי אבטחת מידע בארגון ?

   כן  לא

4. האם קיים מסמך מעודכן של מבנה המאגר כמפורט בתקנה 5 לתקנות אבטחת המידע ?

   כן  לא

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

**אגף מערכות מידע**

**טלפון: 09-8894070**

4/30/2021

ח"מ איר תשפ"א

לכבוד

חב' **מטרופולי-גם בע"מ**

המחזיק מאגר מידע של עיריית הוד-השרון: **מערכת גביה,תיפעל וחנויים העירונית**, מס' _____

א.ג.נ.

**הנדון: תצהיר אבטחת מידע**

בהתאם להוראות התקנות, מחזיק מאגר מידע נדרש לדווח לרשות, אחת לשנה לפחות, אודות אופן ביצוע חובותיו לפי תקנות אבטחת המידע. על כן, נודה לקבלת תשובתכם האם הנכם עומדים בהוראות תקנות אבטחת המידע המפורטות במכתב זה ובאיזה אופן

אבקשכם למלא את השאלון ולהעביר חתום למנהל אבטחת מידע :

**אלכס רקיטה, rakita@hod-hasharon.muni.il , 0505235704**

1. המסק מצהיר כי הוא פועל בהתאם על פי החוק, התקנות וחיקוף הגנת הפרטיות וכי הוא עומד באמצעי אבטחה ובקרה כמתחייב מהוראות חוק הגנת הפרטיות, תיקוניו ותקנותיו והנחיות רשם מאגרי מידע

כן לא

2. האם פנה בארגונך אחראי לאבטחת מידע ?

לא

כן :

שם פרטי_____, שם משפחה_____, תפקיד_____

טל'_____, E-Mail_____

3. האם קיימים נוהלי אבטחת מידע בארגון ?

כן לא

4. האם קיים מסמך מעודכן של מבנה המאגר כמתחייב בתקנה 5 לתקנות אבטחת המידע ?

כן לא

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

**צביקה אליהו - מילאון 92**
tsvika@mileon.co.il
02/05/2021 9:04:50

**RE: שאלון אבטחת מידע**
To: "אלכסנדר רקיטה" <Rakita@hod-hasharon.muni.il>
Copy: "אילן כהן" <IlanC@hod-hasharon.muni.il>

image002.png
image003.png
image004.png

,הי אלכס
קיבלתי, בטיפול

,בברכה
**צביקה אליהו**

| מלאון 92 בע"מ | מנהל לקוחות
סלולר. 050-6007404 | קווי. 073-2010042
אימייל: tsvika@mileon.co.il

http://www.mileon.co.il

**From:** אלכסנדר רקיטה <Rakita@hod-hasharon.muni.il>
**Sent:** Friday, April 30, 2021 1:36 PM
**To:** צביקה אליהו - מילאון 92 <tsvika@mileon.co.il>
**Cc:** אילן כהן <IlanC@hod-hasharon.muni.il>
**Subject:** שאלון אבטחת מידע

**,שלום רב**

**עמידה בהוראות תקנות על בהתאם להוראות התקנות, מחזיק מאגר מידע נדרש לדווח לרשות אבטחת המידע.**

**מצ"ב שאלון בנוגע למצב אבטחת מידע באירגונכם.**

**נודה לכם אם תחזירו אותו מלא וחתום בהקדם האפשרי**

,בברכה

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

אר

**אלכסנדר רקיטה**

30/04/2021 13:25:51

**שאלון אבטחת מידע**

To: irit_ta@malam-payroll.com

Copy: "אילן כהן" <IlanC@hod-hasharon.muni.il>

image001.png | שכר-מלם.pdf

**שלום רב,**

**עמידה בהוראות תקנות על בהתאם להוראות התקנות, מחזיק מאגר מידע נדרש לדווח לרשות אבטחת המידע.**

**מצ"ב שאלון בנוגע למצב אבטחת מידע באירגונכם.**

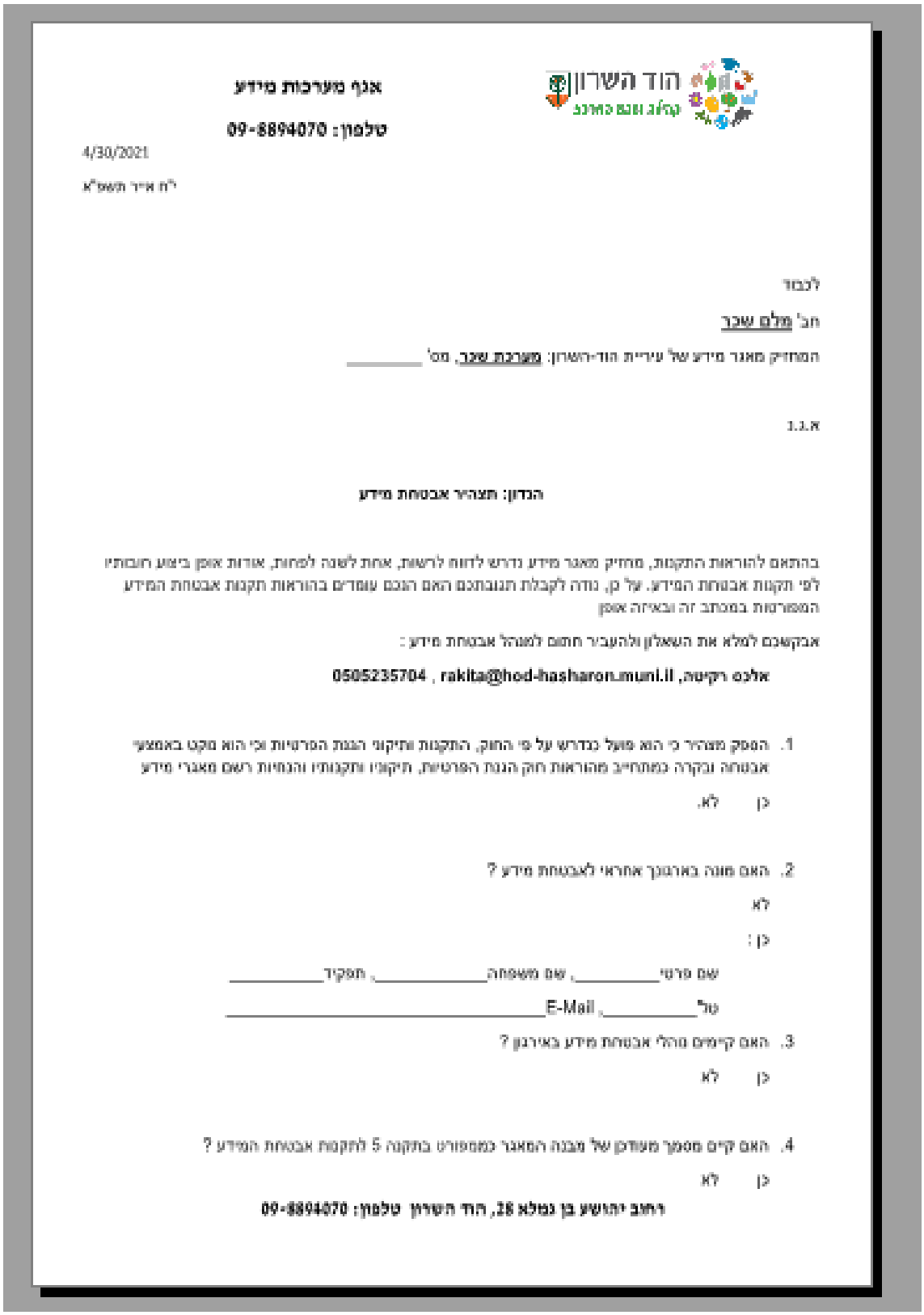
**נודה לכם אם תחזירו אותו מלא וחתום בהקדם האפשרי**

בברכה,

**אלכסנדר רקיטה**
- מנהל אבטחת מידע
אגף מערכות מידע
עיריית הוד השרון

מייל: Rakita@hod-hasharon.muni.il
טל: | נייד: 0505235704

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**



הוד השרון
קהילה ונופש במרכז

**אגף מערכות מידע**

**טלפון: 09-8894070**

4/30/2021

ל"ח אייר תשפ"א

לכבוד

חב' מלם שכר

הנדון: מחזיק מאגר מידע של עיריית הוד-השרון: משרכת שכר, מס' _____

א.ג.נ.

**הנדון: תצהיר אבטחת מידע**

בהתאם להוראות התקנות, מחזיק מאגר מידע נדרש לחוות לרשות, אחת לשנה לפחות, אודות אופן ביצוע חובותיו לפי תקנות אבטחת המידע. על כן, נודה לקבלת תגובתכם האם הנכם עומדים בהוראות תקנות אבטחת המידע המפורטות במכתב זה ובאיזה אופן

אבקשכם למלא את השאלון ולהעביר חתום למנהל אבטחת מידע :

**אלכס רקיטה, rakita@hod-hasharon.muni.il , 0505235704**

1. המסק מצהיר כי הוא פועל בנדרש על פי החוק, התקנות ותיקוני הצנת הפרטיות וכי הוא מקט באמצעי אבטחה ובקרה כמתחייב מהוראות חק הגנת הפרטיות, תיקוניו ותקנותיו והנחיות רשם מאגרי מידע

כן לא.

2. האם מנה בארגנך אחראי לאבטחת מידע ?

לא

כן :

שם פרטי_____, שם משפחה_____, תפקיד_____

טל'_____, E-Mail_____

3. האם קיימים מנהלי אבטחת מידע באירגן ?

כן לא

4. האם קים מסמך מעודכן של מבנה המאגר כמפורט בתקנה 5 לתקנות אבטחת המידע ?

כן לא

**רחוב יהושע בן נמלא 28, הוד השרון טלפון: 09-8894070**

**ע י ר י י ת הוד השרון**

**התחייבות ספקים לשימוש במאגר מידע**

הואיל, ואנו החתומים מטה (להלן: "הספק") נותנים לעיריית הוד השרון (להלן: "העירייה") את השירותים הבאים_____

במאגר מידע: _____ מס: _____

והואיל, ומתן השירותים לעירייה מותנה בהתחייבות שלנו לשמור על סודיות המידע של העירייה ועל אבטחת מידע כמפורט בכתב זה.

**אי לכך, אנחנו מתחייבים בזאת כדלקמן:**

1. הנחיות כללית:

1.1 הספק מצהיר כי הוא פועל כנדרש על פי החוק, התקנות ותיקוני הגנת הפרטיות וכי הוא נוקט באמצעי אבטחה ובקרה כמתחייב מהוראות חוק הגנת הפרטיות, תיקוניו ותקנותיו והנחיות רשם מאגרי מידע.

1.2 הספק מתחייב לדווח לעירייה אחת לשנה לפחות, אודות אופן ביצוע חובותיו לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "תקנות אבטחת מידע").

1.3 הספק ימנה אחראי לאבטחת המידע וסייבר מטעמו. על אחראי אבטחת המידע וסייבר להבטיח שימוש נכון בזיהוי המשתמש ובסיסמא, בהרשאות הגישה למידע ובהגנת משאבי מערכות המחשב והמידע ומערכות התקשורת המכילות מידע השייך לעירייה.

1.4 הספק מתחייב להחתים את עובדיו על הצהרות סודיות, הכוללות, בין היתר, התחייבות לשמירה מוחלטת על סודיות המידע של העירייה, שימוש במידע של העירייה בהתאם לאמור בהסכם בין העירייה לספק ויישום אמצעי האבטחה הקבועים בהסכם.

1.5 הספק מתחייב לא להעביר לצד שלישי מידע שיתקבל במסגרת ההתקשרות, או להשתמש במידע שעובדיו יחשפו אליו אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות ולשמור את המידע במערכת כל עוד נמשך השירות ופרק זמן של עד 90 יום שאותו תגדיר העירייה במועד סיום ההתקשרות.

1.6 הספק מתחייב לאפשר לנציג העירייה לערוך ביקורת אבטחה בכל עת.

1.7 הספק יגדיר נוהל אבטחת מידע, כאמור בתקנה 4 לתקנות אבטחת מידע וכן מסמך מעודכן של מבנה המאגר, בהתאם למפורט בתקנה 5 לתקנות אבטחת מידע.

1.8 הספק יתקין תוכנת הגנה תקנית ומעודכנת נגד נוזקות על מחשבים המכילים מידע השייך לעירייה. הספק לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, ללא אישור מהעירייה וללא התקנת אמצעי הגנה מתאימים.

1.9 הספק ינקוט אמצעי אבטחה הולמים, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת או אל קווי התקשורת בין העירייה אל הספק (לכל הפחות - Firewall ו-IPS, הצפנת TLS 1.2).

1.10 הספק יוודא קיום נהלי התמודדות עם אירועי אבטחת מידע ובכלל זה יקבע הוראות להתמודדות עם אירועי אבטחת מידע, לרבות לעניין ביטול הרשאות וצעדים מיידים אחרים הנדרשים. כמו כן, הספק ינהל ויתעד כל אירוע המעלה חשש לפגיעה במידע או חריגה מהרשאות הגישה במערכות המידע. וישמור את התיעוד באופן מאובטח ולמשך 24 חודשים לכל הפחות.

1.11 הספק ידווח לעירייה על אירועי אבטחה ועל הפעולות שננקטו בעקבותיהם וכן יקיים דיון ויבחן את הצורך בעדכון נוהל האבטחה שלו במאגרי מידע שחלה עליהם רמת אבטחה בינונית, אחת לשנה לפחות. במאגרים שחלה עליהם רמת אבטחה גבוהה, אחת לרבעון לפחות.

1.12 הספק יספק הרשאות גישה, זיהוי ואימות של עובדיו למאגר בהתאם לרמת סיווג ורגישות המאגר, רק לאחר נקיטת אמצעים סבירים, המקובלים בהליכי מיון ושיבוץ עובדים (למשל בדיקות רקע, מבחני אמינות וכיו"ב) וניהול ורישום של בעלי הרשאות גישה יכללו הגדרות של Need to Know ואת המינימום הנדרש לביצוע עבודתם. ניהול דו"ח הרשאות מעודכן הכולל תפקידים, הרשאות הגישה שניתנו ובעלי ההרשאות הממלאים תפקידים אלה, תיעוד כל שינוי בדו"ח, ויכולת הפקה יזומה של דו"ח זה אחת לשנה והעברתו לעירייה.

1.13 הספק יעשה שימוש במדיניות סיסמאות מורכבות והחלפת סיסמא תתבצע לכל הפחות אחת ל-180 יום. הספק יוודא הצפנת סיסמאות בהצפנה חד כיוונית בבסיס הנתונים. כמו כן, הספק יגדיר מספר ניסיונות הקשה שגויים של סיסמא בטרם נעילת המשתמש, יגדיר את אופן הטיפול בתקלות הקשורות באימות זיהוי ויישם ניתוק אוטומטי לאחר פרק זמן של אי פעילות במחשב.

1.14 הספק ידאג לביטול הרשאות לבעל הרשאה שסיים את תפקידו ובמידת האפשר לשינוי סיסמאות למאגר שבעל ההרשאה עשוי לדעת, מיד עם סיום תפקידו.

1.15 הספק יקיים הדרכות לעובדיו בעלי הרשאות גישה למידע המצוי במאגר המידע, בטרם מתן ההרשאות או בטרם שינוי ההרשאות הקיימות. ההדרכות יכללו את החובות לפי חוק הגנת הפרטיות, התשמ"א-1981 ותקנות אבטחת המידע ומסירת מידע אודות חובות בעלי ההרשאות לפי החוק ולפי נוהל האבטחה של הספק.

1.16 בנוסף, הספק יקיים הדרכה תקופתית לבעלי ההרשאות בנושא נוהל האבטחה של הספק והוראות אבטחת המידע לפי החוק ותקנות אבטחת המידע ובדבר החובות של בעלי ההרשאות לפיהם. ההדרכה תיערך לכל הפחות אחת לשנתיים ובהסמכה של בעל הרשאה לתפקיד חדש, סמוך ככל האפשר למועד הסמכתו.

1.17 הספק ייתן מענה אנושי לטיפול באירועי אבטחת מידע וסייבר וידווח על האירועים ועל מסקנותיהם לממונה אבטחת המידע בעירייה.

1.18 הספק יסדיר את גישת העובדים למאגר המידע מרחוק באמצעות זיהוי מבוסס שם וסיסמא לצפייה במידע והזדהות חזקה לביצוע פעולות.

1.19 הספק יגביל ככל הניתן את התקנים ניידים למאגרי המידע (dok, smartphone, laptop)

1.20 הספק יבצע בקרות פלט וקלט.

1.21 הספק יעשה שימוש במערכות הפעלה וגרסאות תוכנה הנתמכות ע"י היצרן, וכן קיום עדכונים שוטפים של מערכות ותשתיות המאגר, לרבות חומר המחשב הנדרש לפעולתן.

**2. דרישות אבטחה נוספות נדרשות על מאגרי מידע ברמת סיווג בינונית וגבוהה:**

2.1 הספק ישמור את מאגרי המידע ואת התשתיות והמערכות המשמשות את המאגרים במקום מוגן המונע חדירה וכניסה אליו ללא הרשאה, יתעד את הכניסות והיציאות ממתקני המאגר, ויתעד הכנסה והוצאה של ציוד על מנת לבצע מעקב ובקרה במקרה של כשל אבטחתי.

2.2 הספק ינהל מנגנון תיעוד אוטומטי (AD) שיאפשר בקרה וביקורת על הגישה למערכות המאגר, התיעוד יישמר למשך שנתיים לפחות. כמו כן, ידאג הספק לקיום נוהל בדיקה שגרתי של נתוני התיעוד כולל דוח של הבעיות שנתגלו והצעדים שננקטו בעקבותיהן.

2.3 הספק יבצע ביקורת תקופתית לכל הפחות אחת ל 24 חודשים, אשר תכלול דו"ח עם זיהוי ליקויים והצעת תיקונים לליקויים אלה.

2.4 הספק יקבע נהלי עבודה לגיבוי ושחזור הנתונים, ויספק על פי הצורך תיעוד לכך. שמירת הגיבויים תיעשה באופן מאובטח ולמשך 24 חודשים לכל הפחות.

2.5 הספק יעדכן את בעל המאגר ואת רשם מאגרי מידע באופן מידיי על אירוע אבטחה חמור, שבו נעשה שימוש **בחלק מהותי ממאגר המידע בלא הרשאה או בחריגה מהרשאה או שנפגעה שלמות המידע במאגר.**

2.6 הספק יבצע סקר סיכונים ומבדק חדירה למערכות מאגרים שחלה עליהן רמת אבטחה גבוהה, אחת ל-18 חודשים לכל הפחות.

**ולראייה באנו על החתום**

| | | | |
|---|---|---|---|
| _____ | _____ | _____ | _____ |
| חברה | שם (משפחה ופרטי) | חתימת הספק | תאריך |

## טופס חתימה אבטחת מידע לספק תוכנה

**<u>התחייבות ספק תוכנה לאבטחת מידע</u>**

הואיל; ואנו החתומים מטה (להלן; "הספק") נותנים לעיריית הוד השרון (להלן; "העירייה") שירותי פיתוח ו/או תחזוקת תוכנה.

והואיל; ומתן השירותים לעירייה מותנה בהתחייבות שלנו לשמור על סודיות המידע של העירייה ועל אבטחת מידע כמפורט בכתב זה;

**אי לכך, אנחנו מתחייבים בזאת כדלקמן;**

1. הנחיות כללית:

1.1 הספק מצהיר כי הוא פועל כנדרש על פי החוק, התקנות ותיקוני הגנת הפרטיות וכי הוא נוקט באמצעי אבטחה ובקרה כמתחייב מהוראות חוק הגנת הפרטיות, תיקוניו ותקנותיו והנחיות רשם מאגרי מידע.

1.2 הספק ימנה אחראי לאבטחת המידע וסייבר מטעמו. על אחראי אבטחת המידע וסייבר להבטיח שימוש נכון בזיהוי המשתמש ובסיסמא, בהרשאות הגישה למידע ובהגנת משאבי מערכות המחשב והמידע ומערכות התקשורת המכילות מידע השייך לעירייה.

1.3 הספק מתחייב להחתים את עובדיו על הצהרות סודיות, הכוללות, בין היתר, התחייבות לשמירה מוחלטת על סודיות המידע של העירייה.

1.4 הספק מתחייב לא להעביר לצד שלישי מידע שיתקבל במסגרת ההתקשרות, או להשתמש במידע שעובדיו יחשפו אליו אגב ביצוע ההתקשרות, לכל מטרה אחרת שלא קשורה לביצוע ההתקשרות.

1.5 הספק מתחייב לאפשר לנציג העירייה לערוך ביקורת אבטחה בכל עת.

1.6 הספק יתקין תוכנת הגנה תקנית ומעודכנת נגד נזקות על מחשבים המכילים מידע השייך לעירייה.

1.7 מנהל אבטחת המידע והסייבר של העירייה יוודא שקוד המקור עבר בדיקה נגד חשיפות ואי קיום קוד זדוני באמצעות סריקת חשיפות אבטחת מידע ( Vulnerability Scan).

1.8 הספק יבצע הדרכה פרונטלית על התוכנה על פי דרישת העירייה.

2. פיתוח מאובטח:

2.1 שימוש בתקן OWASP או מקביל שיאושר ע"י מנהל אבטחת המידע והסייבר של העירייה.
2.2 שימוש בגרסאות מעודכנות ונתמכות של שפות הפיתוח.
2.3 העברת מסמך אפיון מערכת לאישור של מנהל אבטחת מידע וסייבר של העירייה.
2.4 פיתוח המערכת בהתאם לדרישות האפיון.
2.5 ביצוע בדיקות מסירה ע"י הספק לווידוא קיום דרישות אבטחת מידע באפיון.
2.6 מבדק חדירה למערכת לפני העברה לייצור.

3. הגנה אפליקטיבית:
3.1 שימוש בפרוטוקול Https בכל דפי היישום.
3.2 הגדרת רשימת ערכים וטווחים מותרים לשדות קלט (כולל הגנה על FORM באמצעות CAPTCHA)
3.3 מניעת אפשרות למניפולציה של כתובת ה-URL (חוסר יכולת לשנות UID בסוף הדף, לא ניתן לשנות או להוסיף דפי משנה).
3.4 אין לחשוף למשתמש הקצה הודעות שגיאה אפליקטיביות העלולות להסגיר קוד וטבלאות בתוך היישום. שגיאות כאלה יכתבו לקובץ לוג בלבד או לתת הודעה גנרית.
3.5 במקרה של העלאת קבצים למערכת: יש לוודא כי קובץ העולה לשרת יעבור סניטציה ויישמר בשרת כקובץ בעל סיומת לא פוגענית כגון html ו/או php.
3.6 שמירת המידע במערכת כל עוד נמשך השירות.
3.7 בקרת פלט:
3.7.1 וידוא שאין בדו"חות המופקים מהמערכת, חשיפה של שדות שלא נדרשים.
3.7.2 תיוג פלט בעל מידע רגיש המופק מהמערכת כמכיל מידע מוגן/חסוי לפי חוק הגנת הפרטיות.
3.8 תיעוד בלוג:
3.8.1 נעילות משתמש.
3.8.2 פעולות עדכון ע"י המשתמשים כולל שמירת ערך קודם.
3.8.3 העלאות תכנים.

3.9 הזדהות והרשאות:
3.9.1 קישור ל-AD או שימוש במדיניות סיסמאות בה אורך סיסמא מינימלי 7 תווים, מתבצע שימוש באותיות וספרות.
3.9.2 הסיסמאות תוחלפנה לפחות כל 3 חודשים.
3.9.3 הסיסמאות יוצפנו בהצפנה חד כיוונית בבסיס הנתונים.
3.9.4 יכולת להגדיר הרשאות על פי פרופיל ומידור גישה/עדכון ברמת שדה.
3.9.5 יכולת הפקה יזומה של דו"ח הרשאות תקפות אחת לשנה.
3.9.6 יישום תיעוד לכל שינוי בטבלת ההרשאות.
3.10 הפרדת סביבות:

3.10.1 סביבת הייצור תופרד מסביבות אחרות.

3.10.2 העברת אפליקציה מסביבת פיתוח לייצור תתבצע בצורה מבוקרת.

3.10.3 לא יעשה שימוש בנתונים אמתיים בסביבת הפיתוח.

4. דרישות במקרה של פעילות בענן:

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

4.2 שימוש בגרסאות דפדפנים נתמכות.

4.3 ממשק ניהול בגישה מהעירייה בלבד או מכתובות שיסופקו על ידה.

4.4 במקרה של ניהול בענן- מימוש IPS.

4.5 מימוש הצפנה בתקשורת באמצעות פרוטוקול TLS1.2 או פרוטוקול אחר שיאושר ע"י מנהל אבטחת מידע וסייבר של העירייה

4.6 בקרת גישה:

4.6.1 גישה לאפליקציה באמצעות שם משתמש וסיסמא – לאפשר יכולת שימוש ב-OTP או CAPTCHA כמזהה נוסף.

4.6.2 הגדרת SESSION TIME OUT לאחר פרק זמן של אי פעילות, המחייב זיהוי מחדש של המשתמש.

4.6.3 ברירת המחדל לסיום Session תהיה 30 דקות (גם אם המערכת תנוהל מקומית).

4.7 אבטחת תשתיות

4.7.1 הגנת בסיס הנתונים והקשחתו על פי הנחיות העירייה

4.7.2 ניטור שינויים בבסיסי הנתונים והפקת דו"ח לעירייה לפי דרישתה.

4.7.3 זמינות מלאה- מקסימום DOWNTIME – שעה.

4.7.4 שמירת המידע כל עוד נמשך השירות.

4.7.5 הספק יספק לעירייה יכולת שליטה ובקרה על הנתונים בענן וכן אפשרות חד צדדית להפסקת השימוש בשירותי הענן תוך מחיקת המידע באופן שלא ניתן לאחזור.

4.7.6 מענה אנושי לטיפול באירועי סייבר.

**ולראיה באנו על החתום**

| | | | |
|---|---|---|---|
| _____ | _____ | _____ | _____ |
| ספק | שם (משפחה ופרטי) | חתימת הספק | תאריך |

# נספח שמירת סודיות ואבטחת מידע

## 1. שמירת סודיות

1.1. הקבלן מתחייב לשמור בסודיות כל מידע עסקי, תפעולי, מנהלי או אחר הנוגע לעירייה, לתושביה, לקבלניה, לנאשמיה, לעסקיה, לפעילותה, לקניינה הרוחני או האחר, שיגיע אליו, אגב, בקשר או במהלך ביצוע הוראות הסכם זה, ולאחסנם במקום ובאופן המתאים ביותר, לשם שמירת סודיותם כאמור ולא למוסרם בין במישרין ובין בעקיפין לכל אדם ו/או גוף אחר.

1.2. ההתחייבות לשמירה על סודיות לפי סעיף קטן 1 לעיל לא תחול על:

1.2.1. מידע שהינו בבחינת נחלת הכלל במועד מסירתו.

1.2.2. מידע שהיה ברשות הקבלן לפני מסירתו לו על ידי העירייה.

1.2.3. מידע או כל חלק ממנו אותו יידרש הקבלן לגלות, על פי דין, ובלבד שבמקרה כזה יודיע הקבלן לעירייה, תוך זמן סביר, על דבר הדרישה ויעשה כמיטב יכולתו על מנת להותיר בידי העירייה שהות סבירה להתגונן בפני דרישה כזאת.

1.3. הקבלן מתחייב כי כל מידע אשר יוזן למערכת יעמוד בדרישות לאבטחת מידע כמפורט בנספח זה להלן.

1.4. הקבלן מתחייב לבצע את כל דרישות הבטיחות שתידרשנה על ידי העירייה, לרבות כל בדיקה לגבי עובדי הקבלן שתדרוש העירייה.

## 2. אבטחת מידע

2.1. אבטחת המידע במערכות תבוצע בהתאם לחוק הגנת הפרטיות, התשמ"א 1981 ותקנות הגנת הפרטיות (אבטחת מידע) 2018 רמת אבטחה בינוני – בעירייה מאגר באבטחה גבוהה. ממליצה לא לציין אלא להשאיר פתוח כך שיהיה בהתאם לרמת אבטחת מידע הנדרשת להתקשרות גם למקרה שהנתונים גדלים.

2.2. המידע המאוחסן במאגרי הנתונים של המערכות יהיה **חסוי**. נותן השירותים הינו אחראי להקמת והתקנת כל האמצעים הדרושים לשמירת חיסיון הנתונים בפני גורמים שאינם רשאים למידע או חלק מהמידע. נותן השירותים מתחייב ליישם באתריו מערכות לאבטחת מידע, וליישם נהלים והוראות לעניין הגנה על שלמות מידע, הגנה על מידע מפני חשיפה, שימוש או העתקה ללא רשות אחזור מידע וגיבוי נתונים.

2.3. נותן השירותים מתחייב להקפיד על אבטחת המידע שהועבר לרשותו, לאבטח את כל המידע שהגיע אליו במסגרת ביצוע הפרויקט והשירותים לפי הסכם זה, ולוודא **שלא ייעשה במידע הנ"ל כל שימוש מחוץ לזה הקבוע בהסכם**.

2.4. בתום ההתקשרות נותן השירותים יעביר את כל הנתונים לאגף מערכות מידע של המזמין בפורמט ובדרכים מתואמים ויוודא השמדת כל הקבצים והרישומים של כל הפעולות בתוכניות השונות, אלא אם יידרש אחרת על ידי המזמין. בהתאם להוראה בכתב של המזמין.

2.5. נותן השירותים יעמיד יכולת ריכוזית לשליטה בקיום מדיניות אבטחת המידע המפורטת לעיל. ידווח מדי שנה על קיום אבטחת מידע.

2.6. על פי דרישת המזמין יציג הספק לנציג המזמין את אמצעי האבטחה שננקטה.

2.7. עקרון אבטחת המידע של מערכות המידע יתבסס על התפיסה לפיה כל הגישות למידע תהיינה אסורות, פרט לאלו שיוגדרו במפורש כגישות מותרות. ניהול אבטחת המידע ישקף את כללי אבטחת המידע של המזמין, ויכלול ניהול הרשאות ומידור מסמכים.

2.8. ניהול ההרשאות יתמוך בתהליך הגדרת המשתמשים וקביעת ההרשאות לכל משתמש או לכל קבוצת משתמשים (הרשאות מבוססות תפקיד). המערכות תאפשר שכפול פרופיל ההרשאות של משתמש אחד למשתמש אחר.

2.9. ההרשאות תהיינה ברמות שונות, כגון:

2.9.1. שדה - לאילו שדות בכלל התפריט / מסך רשאי המשתמש לגשת.

2.9.2. תפריט - לאיזה תפריטים רשאי המשתמש לגשת, ואיזה תהליכים הוא רשאי להפעיל מאותו תפריט.

2.9.3. תכנית - איזה תכניות ופונקציות רשאי המשתמש להפעיל.

2.9.4. קבצים וחשבונות - לאיזה קבצים/תיקיות וחשבונות מותר למשתמש לגשת.

2.10. במערכות ההרשאות יוגדר מה המשתמש רשאי לבצע בנתונים, דהיינו: צרופים אפשריים של צפייה, עדכון, ביטול, הפעלה וכד' (כגון צפייה בלבד או קריאה ועדכון). ההרשאות יאכפו בכל אמצעי הגישה למערכות, בין אם בטפסים בממשק משתמש, מנגנוני חיפוש, דוחות, גישות ממוכנות באמצעות Web Services וכיו"ב.

2.11. מבלי לגרוע מהאמור לעיל, אבטחת המידע צריכה להסתמך על אבטחה של הגישה לנתונים השמורים. נותן השירותים מתחייב למנוע גישה של לא מורשים למערכת ולמידע של המזמין ולקיום דרישות חוק הגנת הפרטיות. נותן השירותים מתחייב להודיע למזמין בכתב מידע כשהוא יודע על כל מקרה של פגיעה או ניסיון לפגיעה באבטחת המידע.

2.12. שינוי בהרשאות יתבצע בכפוף לפניה מהמזמין בכתב בלבד החתומה ע"י גורמים רלוונטיים.

2.13. לוג פעילויות המערכת יהיה מוגן משינויים.

2.14. נותן השירותים יהיה אחראי למניעת ניסיונות לפגיעה במידע, כל עוד מידע זה נמצא ברשותו או נגיש לו, לעובדיו או לקבלני המשנה שלו או למי מטעמו.

2.15. המערכת יישמרו בקובץ לוג את כל ניסיונות הגישה למערכות, המורשים והבלתי מורשים.

2.16. המערכות יתריעו על כל שינוי בפרמטרים תפעוליים או אבטחתיים. יוגדר משתמש חוץ מערכתי אשר יקבל את ההתרעות.

2.17. המערכות יתריעו לגורם הנ"ל על כל ניסיון חריגה מגישות מורשות או ניסיון לבצע פעולות לא מורשות.

2.18. כאירוע של ניסיון פגיעה במידע או אירוע של פגיעה במידע יוגדרו בין היתר:

2.18.1. כל גילוי של שימוש לרעה במערכות או במידע שבהן.

2.18.2. חדירה לא מורשית למערכות או ניסיון לחדירה כזו.

2.18.3. הכנסות וירוס מחשבים או תוכנת "סוס טרויאני" למערכות.

2.18.4. כל שיבוש או מחיקת מידע לא מורשית.

2.18.5. כל פעולה או ניסיון לבצע פעולה הגורמים להפסקת השירות.

2.18.6. העברת מידע לגורם "לא מורשה".

2.18.7. התחברות או חיבור ציוד לא מורשים לקווי התקשורת של המערכות.

2.19. בעת אירוע במ"מ הממונה על אבטחת המידע מטעם נותן השירותים יבצע תחקיר ראשוני וידווח לממונה על המערכות בסוכנות.

2.20. על הממונה על אבטחת המידע מטעם נותן השירותים לבצע תחקיר מלא תוך 24 שעות עבודה לכל המאוחר, וזאת בהתחשב בחומרת הפגיעה במאגר המידע, וכן לתקן את כל הטעון תיקון על חשבונו באופן מיידי ולא יאוחר מ-24 שעות מעת גילוי האירוע, ולדווח על כך לממונה על המערכות בסוכנות מיד עם השלמת התיקון.

2.21. נותן השירותים אחראי למניעת שיבוש הנתונים, העברתם שלא ברשות, שינויים שלא לצורך, פגיעה בשלמותם וכל פעולה שעשויה לפגוע במי מהגורמים מהם נאגרו הנתונים עפ"י חוק. הגדרות אבטחת מידע אלו תקפות לגבי כל רכיבי התוכנות, מתוכניות גזירת הנתונים ועד יישומי הקצה להצגתם.

2.22. נותן השירותים יישא בכל אחריות במקרים של גילוי ושימוש במידע הקשור למזמין הנמסר על ידו, והנובע מחדירות בלתי מורשות של אחרים.

2.23. אבטחה בתוכנה - האבטחה בתוכנה תתבסס על הפעלת תוכנה לאבטחת מידע, שתבטיח:

2.23.1. מערך הרשאות וסיסמאות לזיהוי כל התחברות למערכות.

2.23.2. דיווח על ניסיונות חדירה לא מורשים למערכות.

2.23.3. דיווח על ניסיונות פגיעה בנתונים.

2.24. מובהר כי דרישות אבטחת מידע בתוכנה ייבדקו כחלק מבדיקות הקבלה של המערכות.

2.25. המזמין או מי מטעמו רשאי לבצע מבדקי חדירה שוטפים לרכיבי המערכות השונים בכדי לבחון את רמת החסינות שלהם לפריצה ומניפולציה ברמת האפליקציה (למשל SQL Injection). נותן השירותים מתחייב לתקן כל חולשת אבטחת מידע שיתגלו במבדקי החדירה.

2.26. על נותן השירותים לבצע בדיקת שחזור נתונים של קלטת הגיבוי לפחות פעמיים בשנה.

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

**נספח כ"ז**



**<u>הנדון : דוח סטטוס – אבטחת מידע הוד השרון</u>**

1. ממצאי דוח סטטוס מתבססים , על מיפוי ראשוני שבוצע על ידי בעירייה , על ממצאי תחקיר אירוע סייבר שבוצע ע"י אגף הסייבר , ועל סקר סיכונים שבוצע בעירייה בשנת 2018.

2. **<u>ממצאים:</u>**

2.1שרת שירות פסיכולוגי - מערכת הפעלה 2003 – ומערכת לא מעודכנת – נדרש בהקדם לשדרג את השרת למערכת הפעלה עדכנית יש להסדיר את נושא הרישוי ושדרוג מערכת המידע העירייה קבילה מבית התוכנה הצעת מחיר לשדרוג.

2.2 תחנות העבודה LOCAL ADMIN - מוגדרות סיסמאות פשוטות – מומלץ להפעיל LAPS.

2.3 תחנות עבודה משתמשים ב DOMIAN מוגדרים כ -LOCAL ADMIN - מומלץ לבטל בהקדם. הרשאות ניהול יהיו מוגבלות לצוות IT בלבד , חריגות יבחנו בקפידה ובמידת האפשר יהיו תחת ניטור. בכל מקרה, משתמשים בעלי הרשאות ניהול לא יבצעו התחברות לרשת באמצעות הרשאות אלה, ההתחברות תתבצע באמצעות משתמש "פשוט" . ובעת הצורך יעשה באופציה שלRun as Administrator.

2.4 להוציא domain users מקבוצת DOMAIN ADMINS - במיידי , אסור שמשתמש בארגון יהיה בעל הרשאות ADMIN ב DOMAIN , מהווה חשיפה לפגיעות על כלל הארגון. לייצר שני משתמשים שונים, האחד לניהול המערכת והשני לעבודה השוטפת.

2.5לא ברורה מדיניות חסימת אתרים, קבצים והורדות מהאינטרנט מבקש לקבל את פירוט החסימות המופעלות על גלישת האינטרנט בעירייה. מאחר והחסימה היא בתצורת PROXY שמוגדרת ב POLICY מחשב שלא מחובר ל DOMAIN אבל מחובר לרשת מקבל גלישה חופשית ללא מגבלות. כמו כן יש לנעול ב GPO את האפשרות למשתמשים לבטל את הגדרות ה PROXY .

2.6 מבקש לקבל שרטוט טופולוגיה של רשת המחשבים בעירייה , ופירוט התעבורה שיוצאת ישירות מה F.W לרשת האינטרנט.

2.7 יש להעביר פירוט חסימות ותעבורה על קווי התקשורת הנוספים בעירייה , קו למטרו , קו לקומפלוט ורשת IPVPN לאתרים מרוחקים.

2.8 שרת דואר בעירייה EXCHANGE 2010 , מערכת קרובה לתום תקופת התמיכה של חברת MICROSOFT . ממליץ לעבור בהקדם לשירות ענן 365 , הועברו הצעות מחיר לעירייה.

2.9 יש בעירייה חוסר ברישוי ל OFFICE , יש לפעול מול MICROSOFT להסדרת הרישוי בעירייה.

2.10 שדרוג שרתי DC בעירייה יש שני שרתי DC 2008 – נדרש לשדרג את מערכת ההפעלה , רכישת רישוי , בניית גיבוי בין שרתי ה DC לשירות ה DHCP – הועברה לעירייה הצעת מחיר לביצוע.

2.11 שירות VPN בעירייה לא מוגדר בתצורת OTP – הועברה הצעת מחיר להטמעת OTP+VPN .

2.12 תכנת אנטי וירוס - מבקש לקבל דוח משרת אנטי וירוס. קיים חוסר ברישוי.



13 עדכוני MICROSOFT - מבקש לקבל דוח משרת העדכונים , נכון לכתיבת הדוח לא מופעל בצורה אוטומטית הפצת עדכוני אבטחת מידע לתחנות ולשרתים. מומלץ להגדיר במערכת העדכונים עדכוני תוכנה למוצרי מדף בדגש על GOOGLE , ACROBAT , JAVA ותוכנות מדף נפוצות בעירייה.

2.14 תוכנת השתלטות VNC - לבדוק האם למשתמשים יש הרשאות ADMIN - מומלץ להתקין VNC SERVER - ובניית הרשאות מגבילות. להגביל את אפשרות ההשתלטות רק לצוות ה IT .

2.15 נהלים מבדיקה עולה כי אין בעירייה נהלי אבטחת מידע מאושרים , הועברו סט נהלים (נוהל שימוש במצלמות , נוהל גישה של נותן שירות חיצוני לרשת, נוהל הוראות הגנת מידע , נוהל שינויים , נוהל אחראיות

עובדים) לאישור העירייה. קיים העדר מנגנון ארגוני לניהול אבטחת מידע , לא הוצגו תוכניות עבודה כנדרש בתקנות מאגרי המידע , לא הוצגו תוכניות עבודה בתחום ה SYSTEM , תקשורת וטלפוניה. מנהל ה SYSYTEM ומנהל התקשורת המשמש גם מנהל אבטחת המידע בארגון יציגו כל אחד בתחומו תוכניות עבודה לשנת 2020 ולשנת 2021 , תוכנית העבודה תעמוד בתקנות אבטחת המידע , תהיה מבוססת תקציב או QUICK WINS .

2.16 מסמך מדיניות אבטחת מידע – נדרש לתקף על פי חוק את המסמך אחת לשנה – הועבר נוסח מעודכן לחתימה.

2.17 מאגרי מידע – ממידע הנמצא במשרד המשפטים ישנם 4 מאגרי מידע רשומים , ממיפוי מערכות הליבה בעירייה עולה באופן ברור כי יש חוסר ברישום מאגרי מידע ובנוסף עולה כי המנמ"רית הקודמת בתפקיד רשומה כ מנהלת כלל המאגרים בעירייה , נעשה מיפוי ונדרש להחתים את מנהלי המאגרים החדשים על המאגרים הרשומים והמאגרים שעתידים להירשם.

2.18 לא מופעלת בעירייה מדיניות סיסמאות מורכבת ואף מוגדרת האופציה שהסיסמא של תוקף לא מוגבל לסיסמאות – חייבים במיידי להפעיל סיסמא מורכבת – הועברה למנהל ה SYSTEM שם של מערכת להפצה למשתמשים המאפשרת תפעול עצמאי של החלפה ושינוי סיסמא. מדיניות הסיסמאות תכיל - סיסמא מורכבת, החלפה כל 3 חודשים ,מספר ניסיונות כושלים , מבנה הסיסמא , איסור להגדרת שם המשתמש , ורצפים קלים.

2.19 גיבויים לא הוצג נוהל ומדיניות גיבויים ו -DR - מבקש לקבל דוח גיבויים ופירוט המדיניות , ממליץ לקיים ישיבה לגבי פתרונות לגיבויים ו DR , לשקול את האפשרות לעלות את שרתי העירייה לענן מרכזי המספק עמידה בכל תקנות אבטחת המידע המחייבות , אבטחה פיזית , עמידות , שרידות ורצף תפקודי (המשכיות עסקית). כתיבת תוכנית DRP מנהל ה SYSTEM והתקשורת יציגו את תפיסתם לגבי מדיניות ה DR בארגון , פירוט ויישום.

2.20 טרם נבדקה אבטחה הפיזית של חדר השרתים – האם קיים UPS , גנרטור , מצלמות , כיבוי אש וכו'.

2.21 לנהל נוהל עבודה עם ספקים ולהחתים ספקים על מסמך שמירת סודיות , הועבר נוהל המסדיר את תצורת החיבור לעירייה של נותני שירות.

2.22 סגמנטציה - הפרדה מלאה של סביבת השרתים וסביבת המשתמשים , מנהל התקשורת נדרש להגיש תכנית עבודה מוסדרת להגדרת הפרדת רשתות בעירייה. הפעלת Port protected לכל המתגים בהם התחנות לא צריכות לדבר אחת עם השנייה. חסימת RDP .

2.23 הצפנת מידע – הפעלת BITLOCKER על מחשבים ניידים ועל מחשבים קריטיים/רגישים בארגון.

2.24 ניהול F.W - קבלת דוח פירוט חוקים מוגדרים, הגדרת חוקים חדשים מחייב אישור עפ"י נוהל שנשלח.

2.25 שדרוג כלל השרתים ותחנות העבודה (במישה וישנן) אשר מותקנת בהם מערכת הפעלה ישנה , מנהל ה SYSTEM יציג מתודולוגיית הקשחה לשרתים והמחשבים , הטמעת best practice של הספק.

2.26 העדר מערכת לזיהוי אנומליות ברשת , מומלץ להטמיע מערכת כדוגמת PROMISEC – מנהל התקשות יעשה פנייה לחברת בזק.

2.27 SIEM מערכת ניהול לוגים ואירועים – הועברה הצעת מחיר לעירייה להטמעה וביצוע פיילוט.

2.28 היעדר בקרה על חיבור פיזי לרשת הארגון - הטמעת מערכת NAC , מנהל התקשורת יציג את המשמעיות הטכנולוגיות והפערים אל מול ציוד התקשורת הקיים בעירייה להטמעת מערכת NAC.

2.29 הצעות מחיר ל PT וסקר סיכונים – לקראת סוף השנה ובתאם לתקנות אבטחת המידע יש לבצע סקר סיכונים ומבדק PT בעירייה.

2.30 לתאם הדרכות עם אגף הסייבר של משרד הפנים למנהלי מאגרי מידע ולמשתמשים ומועד נוסף למילוי שאלון בקרות ובניית תכנית עבודה.

2.31 לא הוצגה על ידי מנהל אבטחת המידע תוכנית בקרות מנהלתיות , טכנולוגיות לאבטחת מידע בעירייה.

2.32 מערכות מידע בדיקת הרשאות משתמשים – לא הוצגה תוכנית לבדיקת הרשאות משתמשים במערכות המידע , האם ניתנו בהתאם להגדרת התפקיד , האם המשתמש פעיל וכו' כמתחייב בתקנות אבטחת המידע ובאחריות מנהל המאגר הרלוונטי. נוהל ניוד\עזיבה\קליטת עובד.

2.33 חסימת אתרי MAIL ואחסון חיצוניים , לאפשר שימוש לשליחת מיילים רק במערכת הדואר הארגונית , לאחר הטעמת שרת 365 ומעבר התיבות לענן תותקן מערכת cognni לדלף מידע.

2.34 לא הוצג האם נעשה שימוש בעירייה במערכות שו"ב כדוגמת PRTG , KIWI SYSLOG .

**לשכת מבקר העירייה**
**והממונה על תלונות הציבור**

*רבינוביץ אסף - 0544861640*
*מנהל אבטחת מידע אשכול רשויות השרון*

אגף משכנתאות מידע - 2021