

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 1	

## מדריך הגנה על המידע המועצה להסדר ההימורים בספורט

**מטרת המדריך הינה:**

הצגת תפיסת ההנהלה לגבי ההגנה על המידע במועצה וחיזוק מחויבותה לנושא

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 2	

### פרקי המדריך

1. מנהלה שגיאה! הסימניה אינה מוגדרת.
2. כללי שגיאה! הסימניה אינה מוגדרת.
3. עיקרי מדיניות ההגנה על המידע 6

### אי שורים

תאריך	סימוכין	תפקיד	שם	מהדורה
12.2017		מנהלת אבטחת מידע	אירית אריק	1.0

### רשומות מפתח

מילים לחיפוש: מדיניות, מדריך, אבטחת מידע
--



נהלי אבטחת מידע

דצמבר 2017

בתוקף מ

מדריך ומדיניות הגנה על המידע - טוטו

מתוך 45

עמוד 3

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 4	

## 1. מנהלה

### 1.1 מטרה

1. הצגת תפיסת ההנהלה לגבי ההגנה על המידע במועצה וחיזוק מחויבותה לנושא.
2. קביעת עקרונות מנחים ליישום ההגנה על המידע במועצה על בסיסם ניתן יהיה ליישם אמצעי אבטחה ולאורם ניתן יהיה לבחון את רמת ההגנה הקיימת.
3. העלאת רמת המודעות של עובדי המועצה להסדר ההימורים בספורט לנושאי אבטחת מידע.
4. הגדרת סמכויות להגנה על המידע בחברה.
5. מתן מסגרת לכלים ולתהליכים המרכזיים במועצה בנושאי ההגנה על מידע, תוך יצירת תשתית לנהלים מקיפים בתחומים השונים.
6. הבטחת רציפות הכנסות המועצה בערוצי המכירה השונים ומיקסום ההשקעות.
7. לשמור על סודיות לקוחותיה של המועצה.
8. להגן על אמינות המידע האגור במערכות המועצה.
9. להבטיח את תשלומי הזכיות ללקוחות המועצה.
10. הבטחת שירותי המועצה לפעילות 24/7
11. קיום שיפור מתמיד.

### 1.2 אחריות

#### 1.2.1 אחריות לביצוע המדריך

1. ועדת ההיגוי לנושא הגנה על מידע אחראית לגיבוש עקרונות המדיניות, להתוויית אסטרטגיות לפעילות, לפיקוח אחר תכניות העבודה השנתיות, לקיום הערכת נזקים בעקבות תקלות ולגיבוש המלצות לטיפול.
2. ממונה אבטחת מידע בשיתוף עם מנמ"ר המועצה להסדר ההימורים בספורט אחראים לניהול והנחייה מקצועית שוטפת בתחום אבטחת המידע והנחלתה בשטח של החלטות וסיכומי ועדת ההיגוי להגנה על המידע. ממונה אבטחת מידע אחראי לעדכון נוהל זה עפ"י החלטות וסיכומי ועדת ההיגוי לאבטחת המידע.

### 1.3 תחולה

1. הנחיות מדריך זה תקפות לכלל עובדי המועצה להסדר ההימורים בספורט
2. תחולה התקן הינה על תהליכים, ממשקים וטכנולוגיות במועצה להסדר ההימורים בטוטו.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 5	

#### 1.4 נהלים, תקנים ומסמכים קשורים

1. תקן 27001

מהות השינוי	מאשר	אחראי	תאריך	מהדורה
מסמך מאושר	אלי בן סימון	אירית אריק	12.2017	1.0



נהלי אבטחת מידע

דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 6	

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 7	

## 2. כללי

- פעילותה התקינה של המועצה להסדר ההימורים בספורט מושפעת ותלויה ברמת הסודיות, השלמות, הזמינות, הכלילות (Integrity) ושרידות של נכסי המידע של המועצה להסדר ההימורים בספורט.
- פגיעה במידע תוביל לנזקים העלולים לתת אותותיהם בהיבטים תפעוליים, טכנולוגיים וכספיים, לפגיעה במוניטין ובתדמית המועצה להסדר ההימורים בספורט.
- מדיניות ההגנה על המידע מבוססת על ניהול סיכוני אבטחה הדינמיים תוך התאמה לצרכים התפעוליים והארגוניים של המועצה להסדר ההימורים בספורט. העקרונות המונחים במדיניות ההגנה על המידע מהווים בסיס לנהלי העבודה בתחומי אבטחת המידע השונים.
- מדיניות ההגנה על המידע של המועצה להסדר ההימורים בספורט נגזרת מתקן ניהול אבטחת המידע הבינלאומי ISO 27001 ותקן WLA Security control standard
- מדריך אבטחת המידע כורך בתוכו את מסמך המדיניות, כנספח של המדריך.

## 2.2 הגדרות

המונח	ביאור
מדיניות הגנה על המידע	עקרונות המפורטים במסמך מטעם הנהלת המועצה להסדר ההימורים בספורט בו מצהירה ההנהלה לגבי מחויבותיה בעניין עמידה בכל חוק, תקן ונוהל בהיבט ההגנה על המידע.
מידע	כל נתון הנוגע ו/או הקשור לפעילותה, תפעולה או תפקודה של המועצה להסדר ההימורים בספורט.
אבטחת מידע	מכלול הפעולות והאמצעים הננקטים והמיושמים בחברה, שמטרתם להביא לכך שהמידע, יוגנו מפני פגיעה, חשיפה, מחיקה או שינוי, במזיד או בשוגג, הן מתוך המועצה להסדר ההימורים בספורט והן מחוצה לה.
ועדת ההיגוי לנושא אבטחת מידע	פורום ניהולי המונה את מנכ"ל המועצה להסדר ההימורים בספורט, ממונה אבטחת מידע, מנמ"ר המועצה להסדר ההימורים בספורט, מנהל תשתיות ותפעול ונועד לאשרר ולתקף את מדיניות המועצה להסדר ההימורים בספורט בנושא ההגנה על המידע, להתוות אסטרטגיות לפעילות, לפקח אחר תכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

## 2.3 מטרות אבטחת המידע בחברה

- צמצום הסיכונים העלולים להוביל לפגיעה במידע, במאגריו ובמערכותיו.
- צמצום הסיכונים העלולים להוביל להפסדים כספיים

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 8	

3. מזעור סיכוני הפגיעה בתפעולה הסדיר, במוניטין ו/או בתדמית המועצה להסדר ההימורים בספורט.
4. עמידה בחוקים ובתקנים אליהם מחויבת המועצה להסדר ההימורים בספורט.
5. שילוב אבטחת מידע מעקב, ניטור ובקרה אחרי הפעילות והתהליכים העסקיים.
6. ההנהלה תפעל לשיפור מתמיד ע"י השגת המטרות שהוגדרו ע"י ההנהלה ומדידת השגתן.
7. מדיניות אבטחת מידע והנהלים יהיו מוכרים לכלל העובדים ויפורסמו בpublic FOLDER של הארגון באמצעות מייל עם בקרת אישור.

### 3. עיקרי מדיניות ההגנה על המידע

מדיניות ההגנה על המידע של המועצה להסדר ההימורים בספורט שמה דגש על התחומים המרכזיים הבאים:

#### 3.1 מבנה ארגוני

- להגדיר את המסגרות הארגוניות, אשר יישמו את מדיניות ההגנה על המידע במועצה ויבקרו את אופן יישומה. בפרק זה יוגדרו בעלי התפקידים השונים, וכן יפורטו סמכויותיהם ויחסי הגומלין ביניהם.

#### 3.2 אבטחה פיזית

- הגנה על מכלול הציוד והמידע המצויים באתר המועצה להסדר ההימורים בספורט מפני גישה פיזית של גורמים בלתי מורשים, אשר תוצאותיהן עשויות להיות חשיפה, גניבה, שינוי או הרס של מידע.

#### 3.3 אבטחת רשומות

- הגדרת תהליכי וכלי הטיפול ברשומות (מצעים פיזיים נושאי מידע), במטרה לצמצם את סיכוני הפגיעה במידע האגור בהם.

#### 3.4 אבטחה לוגית

- הגדרת שכבות האבטחה הקיימות בתחומים הלוגיים, המהווים מעגלי הגנה על המידע, בתחומי המחשוב והתקשורת.

#### 3.5 אבטחת מידע משאבי אנוש

- קביעת עקרונות ההגנה על המידע בכל הקשור לעובדי המועצה להסדר ההימורים בספורט ותהליכי הקליטה והעזיבה של עובדים, על מנת לצמצם את הסיכונים הנובעים מחוסר מודעות של עובדים, טעויות אנוש, התנערות מאחריות או רצון מכוון של עובד לפגוע במידע האגור במערכות המועצה להסדר ההימורים בספורט.



		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 9	

### 3.6 ניהול וסיווג נכסים

- להבטיח כי כל נכסי המועצה להסדר ההימורים בספורט ידועים, מסווגים ומנוהלים כראוי, וכי קיים גורם הנושא באחריות לגבי כל אחד מהנכסים.

### 3.7 אבטחת ממשקים עסקיים

- צמצום הסיכונים הנובעים מחשיפה של עובדי חברות חיצוניות למידע ולמערכות של המועצה להסדר ההימורים בספורט.

### 3.8 טיפול באירועי הגנה על מידע

- קביעת עקרונות דיווח וטיפול באירועי הגנה על מידע, באמצעותם ניתן יהיה לצמצם את הנוק שיגרם כתוצאה מהאירועים, תיקון הליקויים, טיפול משמעותי בגורמים הרלוונטיים והפקת לקחים לעתיד.

### 3.9 פיתוח ורכש

- קביעת עקרונות לשילוב אבטחת מידע בתהליכי הפיתוח והרכש, על מנת להבטיח כי ייושמו במערכות המועצה להסדר ההימורים בספורט אמצעי אבטחה מתאימים, בהתאם לרמת הרגישות של כל מערכת.

### 3.10 ניהול המשכיות עסקית

- הגדרת העקרונות שיאפשרו את המשך הפעילות העסקית החיוניות של המועצה להסדר ההימורים בספורט בעת חירום.

### 3.11 תוכנית עבודה ותקציב

- גיבוש תוכנית העבודה והתקציב בתחומי ההגנה על מידע, במטרה לעמוד ביעדים ולנתב משאבים נדרשים.

### 3.12 התאמה (COMPLIANCE)

- להבטיח כי המועצה להסדר ההימורים בספורט עומדת בכל דרישות החוק הישראלי, התקנים והדרישות הנוגעות להיבטי אבטחת מידע להם מחויבת המועצה להסדר ההימורים בספורט. הגדרת הפעילויות והכלים, אשר ישמשו את גורמי אבטחת המידע לבדיקת היישום של מדיניות אבטחת המידע, הנהלים והסטנדרטיים הטכניים במערכות השונות ובקרוב עובדי המועצה להסדר ההימורים בספורט.

- אבטחת המידע במועצה תיושם בכפוף ובצמידות לחוקי מדינת ישראל הנוגעים לתחום אבטחת המידע, לרבות חוק המחשבים, חוק הגנת הפרטיות ותקנותיו, תקן ניהול אבטחת המידע, ת"י 27001/2.

### 3.13 בקרה

- ועדת ההיגוי לנושא ההגנה על המידע תבצע סקירה של ישימות מדיניות אבטחת המידע במסגרת סקר הנהלה.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 10	

- ועדת ההיגוי תאשר במסגרת סקר ההנהלה פרמטרים לבדיקת אפקטיביות מערך האבטחה של המועצה להסדר ההימורים בספורט. הפרמטרים יכללו מדדים כמותיים לבחינת רמת העמידה בפרמטרים המוגדרים.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 11	

## מסמך מדיניות אבטחת מידע

אישור מנכ"ל

שם: \_\_\_\_\_ חתימה: \_\_\_\_\_

נחתם בתאריך: \_\_\_\_\_

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 12	

## תוכן

11	מסמך מדיניות אבטחת מידע
13	1. מקור הדרישה
14	2. הבנת צרכים של בעלי עניין
15	3. מחויבות הנהלה
17	4. תחום יישום
18	5. מבנה ארגוני
21	6. ניהול וסיווג נכסים
22	7. מערך הסיווג
24	8. אבטחת משאבי אנוש
26	9. נהלים
27	10. טיפול באירועי אבטחת מידע
28	11. שימוש בציד המחשוב במועצה
29	12. אבטחת מידע בעבודה מול ספקים חיצוניים ובעלי העניין
31	13. אבטחה פיזית
32	14. אבטחת רשומות
33	15. אבטחה לוגית

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 13	

## 1. מקור הדרישה

- 1.1. מדיניות ההגנה על המידע של המועצה להסדר ההימורים בספורט נגזרת מתקן ניהול אבטחת המידע הבינלאומי ISO 27001/2 ותקן WLA Security control standard ומאפשרת ישור קו אל מול סטנדרטיים בינלאומיים בנושא אבטחת מידע.
- 1.2. העמידה בתקן מתווה דרך סדורה לניהול מערך אבטחת המידע.
- 1.3. פעילותה התקינה של המועצה להסדר ההימורים בספורט מושפעת ותלויה ברמת הסודיות, השלמות, הזמינות, הכלילות (Integrity) ושרידות של נכסי המידע של המועצה להסדר ההימורים בספורט.
- 1.4. פגיעה במידע תוביל לנזקים העלולים לתת אותותיהם בהיבטים תפעוליים, טכנולוגיים וכספיים, לפגיעה במוניטין ובתדמית המועצה להסדר ההימורים בספורט.
- 1.5. מדיניות ההגנה על המידע מבוססת על ניהול סיכוני אבטחה הדינמיים תוך התאמה לצרכים התפעוליים והארגוניים של המועצה להסדר ההימורים בספורט. העקרונות המונחים במדיניות ההגנה על המידע מהווים בסיס לנהלי העבודה בתחומי אבטחת המידע השונים.



## נהלי אבטחת מידע

דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 14	

## 2. הבנת צרכים של בעלי עניין

בעלי עניין	דרישות אבטחת מידע	תקשורת עם בעלי עניין
מהמרים	חוק הגנת הפרטיות	אתר WINNER MOBILE
אגודות ספורט	חוק הגנת הפרטיות	אתר הקצבות
דירקטוריון	תקן 27001	ועדת ביקורת
משרד התרבות והספורט	אגודות ספורט , קרן מתקנים	מפגשי המועצה הלאומית לספורט
משרד האוצר	מפקח על אישור תקנים גיוס כח אדם	חוק המכרזים
בעלי תחנות	חוק הגנת הפרטיות , נהלי אבטחת מידע	השתלמויות
משרד המשפטים והמשטרה	חוק הגנת הפרטיות חוק להסדר ההימורים בספורט	חוק הגנת הפרטיות
חוק הלבנת הון	דרישות אבטחת מידע לאיסור הלבנת הון	חוק הלבנת הון
המועצה הלאומית	אין דרישות מיוחדות	
עובדי המועצה להסדר ההימורים בטוטו	תקן ISO 27001 חוק הגנת הפרטיות חוק להסדר ההימורים בספורט	במיילים , ספריה משותפת המכילה את הנהלים

		<b>נהלי אבטחת מידע</b>
דצמבר 2017	בתוקף מ	<b>מדריך ומדיניות הגנה על המידע - טוטו</b>
מתוך 45	עמוד 15	

### 3. מחויבות הנהלה

3.1. הנהלת המועצה להסדר ההימורים בספורט מחויבת למטרות ועקרונות הגנת המידע המהווים חלק בלתי נפרד מקיומה התפעולי והעסקי של המועצה להסדר ההימורים בספורט.

3.2. הנהלת המועצה להסדר ההימורים בספורט מחויבת לעקרונות מדיניות הגנה על המידע, תוך ניהול והקצאת המשאבים הנדרשים לקיומם ההולם של התהליכים, השיטות והכלים שיוגדרו במועצה, כנגזר ממסמך זה.

3.3. הנהלת המועצה להסדר ההימורים בספורט תפעל לשיפור מתמיד של תשתית ההגנה על המידע, במסגרת פעילות לזיהוי הזדמנויות לשיפור ויישומן.

3.4. הנהלת המועצה להסדר ההימורים בספורט רואה את ההגנה על המידע בהיבט של שלימות, זמינות ואמינות כנושא בעל חשיבות עליונה. על עובדי המועצה להגן, לדווח ולטפל בכל אירוע המסכן את המידע.

3.5. הנהלה רואה במערכת ניהול אבטחת המידע (מנא"מ) את המסגרת הניהולית בה יטופל נושא אבטחת המידע במועצה להסדר ההימורים בספורט ותפעל להצלחתה.

3.6. הנהלה תשלב אבטחת מידע בתהליכים העסקיים ובטכנולוגיות המוטמעים ומשולבים במועצה להסדר ההימורים בספורט

3.7. על מנת לעמוד ביעדים שהציבה לעצמה הנהלה בנושא אבטחת מידע, היא תפעל בדרכים הבאות:

3.7.1. העמדת תקציב ראוי לנושא אבטחת המידע.

3.7.2. מינוי ועדת היגוי לאבטחת מידע אשר תקבע את מדיניות המועצה ותקבל החלטות בנושא אבטחת המידע

3.7.3. מינוי ממונה אבטחת המידע אשר יהיה אחראי על מתודולוגית אבטחת המידע במועצה להסדר ההימורים בספורט וינהל את כלל הפעילויות הנוגעות לאבטחת מידע.

3.7.4. העלאת מודעות העובדים לנושא אבטחת המידע.

3.7.5. שילוב תשומות אבטחת מידע ברכש ובפיתוח של מערכות חדשות.

3.7.6. ביצוע סקרים תקופתיים לבדיקת רמת אבטחת מידע.

3.7.7. הטמעה של טכנולוגיות אבטחת מידע מתקדמות לניטור ומניעה של אירועי אבטחת מידע.

3.8. מדדים למעקב ובקרה ואמת מידה לאימות הישגים:

3.8.1. הנהלה תעקוב אחר מבדקי מנא"מ פנימיים וסטאטוס תיקון ליקויים.

3.8.2. הנהלה תעקוב אחר הטיפול בסיכונים אבטחת המידע.

3.8.3. הנהלה תעקוב אחר סקרי סיכונים ומבדקי חדירה על תשתית החברה

3.8.4. הנהלה תוודא את קיום מבדקי מת"י אחת לתקופה אשר הוגדרה/ תוגדר ע"י הסוקר.

3.8.5. הנהלה תדרוש מממונה אבטחת המידע סטאטוס תקופתי על ניטור ובקרה על המערכות השונות.

3.8.6. הנהלה תבצע סקרי הנהלה אחת לשנה בהתאם לנוהל " סקר הנהלה " .

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 16	

3.9. ועדת ההיגוי תקיים סקרי הנהלה אשר נועדו לבדוק את ישימות וביצוע הפעילויות המוגדרות למערכת ניהול אבטחת המידע של המועצה להסדר ההימורים בספורט. הסקר יבדוק את כלל נושאי אבטחת המידע, לרבות ישימותם של מסמך המדיניות ונהלי אבטחת המידע. תוצאות הסקר יהוו שיקול להטמעת המלצות וביצוע שינויים רלוונטיים.

3.10. ועדת ההיגוי תגבש מדדים כמותיים בנושאי אבטחת מידע, אשר באמצעותם ניתן יהיה לבחון ולמדוד את רמת אפקטיביות יישום תשתית אבטחת המידע. ועדת ההיגוי תגדיר את היעדים הכמותיים הנדרשים ותעמוד על מידת היישום בתום כל שנה לפחות, במסגרת סקר ההנהלה.



		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 17	

#### 4. תחום יישום

4.1. המדיניות חלה על כלל עובדי המועצה להסדר ההימורים בספורט.

4.2. המדיניות חלה על מכירה של משחקי הימורים בספורט בישראל.

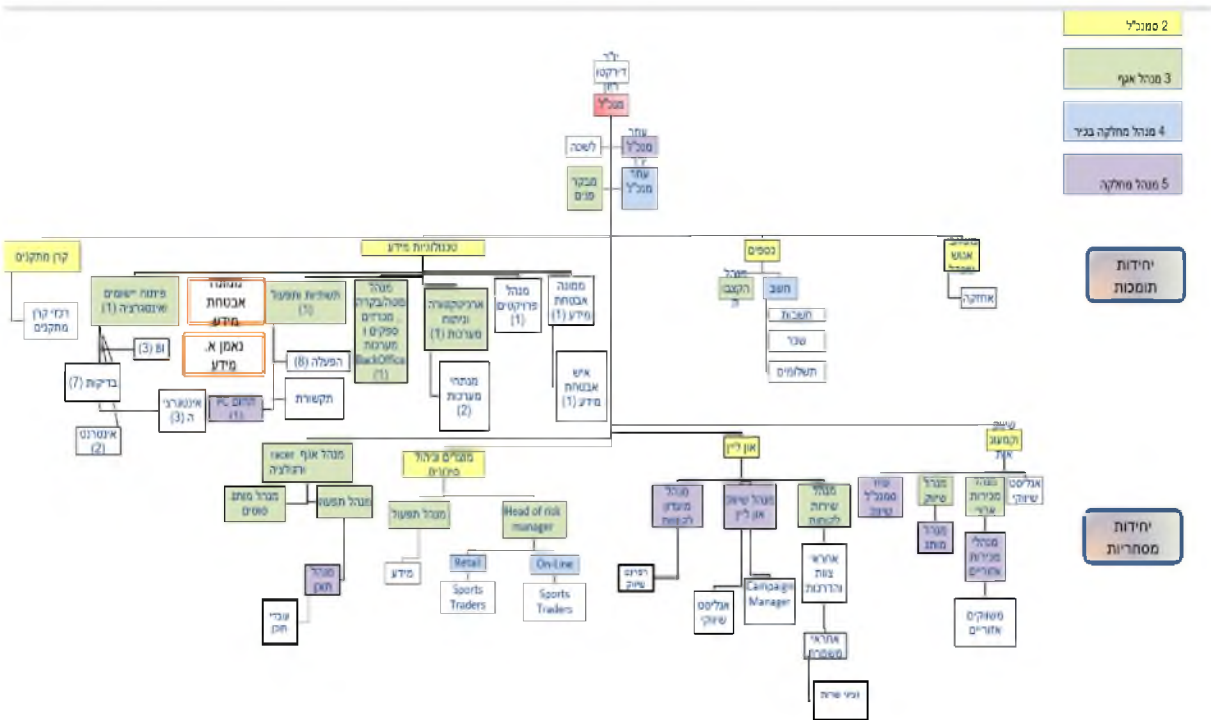
4.3. תהליכי ליבה:

- הגדרת והקמת מחזור משחקי הספורט ומשחקי ההימורים
- פתיחת וסגירת המערכת להימורים
- יצירת מגבלות על סכומי ההימור
- הזנת תוצאות המשחקים למערכת
- ניהול סיכונים - קבלת התראות בזמן ביצוע הימורים – שינוי יחסי הימורים
- ניהול חשבונות לקוחות אינטרנט ומובייל – ממשק משרד הפנים
- זכיות באינטרנט ובמובייל
- זכיות בתחנות
- קרן הקצבות
- קרן מתקנים
- מערכת דיווח נוכחות ושכר עובדי המועצה
- היבטי אבטחת מידע פיזיים

		<b>נהלי אבטחת מידע</b>
דצמבר 2017	בתוקף מ	<b>מדריך ומדיניות הגנה על המידע - טוטו</b>
מתוך 45	עמוד 18	

## 5. מבנה ארגוני

מטרת פרק זה היא להגדיר את המסגרות הארגוניות, אשר תיישם את מדיניות ההגנה על המידע במועצה ויבקר את אופן יישומה. בפרק זה יוגדרו בעלי התפקידים השונים, וכן יפורטו סמכויותיהם ויחסי הגומלין ביניהם.



### 5.1. ועדת היגוי להגנה על המידע

5.1.1. מטרה: יצירת מסגרת ארגונית ניהולית לקבלת החלטות אסטרטגיות בתחום ההגנה על המידע, להתעדכנות בנושאי אבטחת מידע ולביצוע בקרה ניהולית על יישום אבטחת המידע בחברה.

5.1.2. עקרונות פעילות: פורום ניהולי שמונה ע"י מנכ"ל המועצה להסדר ההימורים בספורט ובראשו יושב מנכ"ל המועצה להסדר ההימורים בספורט ונועד לאשרר ולתקף את מדיניות המועצה להסדר ההימורים בספורט בתחום אבטחת המידע, להתוות אסטרטגיות לפעילות, לפקח אחר תכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

5.1.3. חברי ועדת ההיגוי:

- מנכ"ל המועצה להסדר ההימורים בספורט
- מנמ"ר המועצה להסדר ההימורים בספורט
- מנהל תשתיות ותפעול

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 19	

- ממונה אבטחת מידע
- מנהל רגולציה
- במידת הצורך, ובהתאם לנושאים המתוכננים לעלות לדיון מסגרת הוועדה, יזומנו לישיבות גורמים נוספים.

תפקידי ועדת ההיגוי לנושאי אבטחת מידע:

- 5.1.3.1 התוויה של העקרונות והתפיסות הנוגעות להיבטי ההגנה על המידע במועצה.
- 5.1.3.2 אישור מדיניות הגנה על המידע.
- 5.1.3.3 אישור תכנית העבודה בתחום אבטחת המידע ובקרה על יישומה.
- 5.1.3.4 התעדכנות בנושא אירועי אבטחת מידע חריגים שאירעו בחברה.
- 5.1.3.5 התעדכנות בסיכונים ובאיומים הנוגעים למועצה, פיקוח על ניהול הסיכונים המבוצע על-ידי ממונה אבטחת מידע, אישור הסיכונים השיריים וקבלת החלטות באשר לצורך בביצוע שינויים בעקרונות אבטחת המידע.
- 5.1.3.6 קביעת רמות הסיווג של נכסי המידע
- 5.1.3.7 אישור חריגות ממדיניות אבטחת המידע של המועצה להסדר ההימורים בספורט.
- 5.1.3.8 הקצאת משאבים (כסף, כ"א וזמן) ליישום דרישות תשתית אבטחת המידע.
- 5.1.3.9 גיבוי ניהולי של היבטי אבטחת המידע במועצה להסדר ההימורים בספורט.

## 5.2 ממונה אבטחת מידע

- 5.2.1 ממונה אבטחת מידע ישמש גם בתפקיד של מנהל אבטחת מידע
- 5.2.2 ממונה אבטחת מידע יהיה כפוף למנהל מערכות מידע של המועצה להסדר ההימורים בספורט.
- 5.2.3 ממונה אבטחת מידע יבטיח את יישום מדיניות אבטחת המידע בחברה, תוך פריטתה למטלות לביצוע, דרישות, הנחיות, נהלים וכלים טכנולוגיים. להטמיע ולוודא יישום היבטי אבטחת המידע הנוגעים לתחומי המחשוב והתקשורת.
- 5.2.4 תפקידי ממונה אבטחת מידע:
  - 5.2.4.1 ניהול והנחייה מקצועית שוטפת בתחום אבטחת המידע.
  - 5.2.4.2 הנחלה בשטח של החלטות וסיכומי ועדת ההיגוי לאבטחת המידע.
  - 5.2.4.3 הגדרת תוכנית העבודה בתחומי אבטחת המידע וניהול יישומה בשיתוף מנהל טכנולוגיות מידע ומיישם אבטחת מידע של היחידה למערכות מידע.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 20	

5.2.4.4 הגדרת הכלים והתהליכים הנדרשים ליישום היבטי אבטחת המידע וכן ווידוא יישומם.

5.2.4.5 ביצוע בקרה ניהולית שוטפת אחר יישום אבטחת המידע בחברה, ובכלל זה על כל הנגזר ממסמך המדיניות, הנהלים, התקנים והחוקים המחייבים בנושאי אבטחת מידע.

5.2.4.6 תיאום רכש של מוצרים או שירותים, אשר יש ברכישתם השלכות בכל הנוגע לאבטחת המידע בחברה.

5.2.4.7 סיוע בהעלאת מודעות לעובדי המועצה בתחומי אבטחת מידע

5.2.4.8 ייזום סקרי סיכונים וניהול הסיכונים בחברה.

5.2.4.9 ניהול ויישום תוכנית מבדקים פנימיים, אשר יבוצעו על ידו ו/או על ידי מי מטעמו.

5.2.4.10 טיפול בהיבטי אבטחת מידע בקרב ממשקים עסקיים.

5.2.4.11 טיפול באירועי אבטחת מידע.

5.2.4.12 התעדכנות בטכנולוגיות אבטחת מידע ואיתור טכנולוגיות ומוצרים המתאימים לחברה

5.2.4.13 הכנת החומרים לדיון בסקר הנהלה השנתי לאבטחת מידע ברשות המנכ"ל.

5.2.4.14 הוצאה לפועל של החלטות סקר הנהלה השנתי.

5.2.5 דרישות התפקיד :

5.2.5.1 אחוזי משרה משוערים (חודשי) : 60% ל 100% בהתאם לצורך.

5.2.5.2 הכשרות CISO, iso lead auditor

5.2.6 תפקידי נאמן אבטחת מידע :

5.2.6.1 בקרה על תפעול ותחזוקה שוטפים של יישומי אבטחת מידע

5.2.6.2 הטמעה של עקרונות המדיניות, הנהלים, הנחיות עבודה ומתודולוגיות בנושאי אבטחת מידע.

5.2.6.3 ביצוע בקרה שוטפת אחר יישום עקרונות מדיניות ההגנה על המידע והנהלים הנוגעים למערכות השונות.

5.2.6.4 יישום היבטי אבטחת מידע במערכות המועצה להסדר ההימורים בספורט וכן הטמעה ותפעול שוטף של מוצרי אבטחת מידע במערכות..

5.2.6.5 איתור ודיווח על אירועים חריגים.

5.2.7 דרישות התפקיד :

5.2.7.1 אחוזי משרה משוערים (חודשי) : 100%.

5.2.7.2 הכשרות : קורסים והסמכות מקצועיות בתחום אבטחת מידע

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 21	

## 6. ניהול וסיווג נכסים

### 6.1. ניהול נכסי המועצה להסדר ההימורים בספורט

6.1.1. מטרה: להבטיח כי כל נכסי המועצה להסדר ההימורים בספורט נמצאים תחת שליטה, וכי קיים גורם הנושא באחריות לגבי כל אחד מהנכסים.

6.1.2. עיקרי המדיניות:

6.1.2.1. כל נכסי המועצה להסדר ההימורים בספורט ינוהלו במסגרת רשימות מצאי מעודכנות, כאשר עבור כל נכס ימונו "בעלים" (ראה פרק העוסק בבעלי המידע).

6.1.2.2. רשימות נכסי המידע יכללו פירוט הנכס, ציון של בעל הנכס, בעל הסיכון, סיווג הנכס.

6.1.2.3. בעל הנכס יישא באחריות הכוללת לאבטחת הנכס ברמה הנדרשת.

6.1.2.4. ממונה אבטחת מידע יספקו את הכלים והתהליכים לאבטחת הנכס, כנדרש.

6.1.2.5. נכסי המידע במועצה כוללים, בין היתר:

6.1.2.5.1. מאגרי מידע רגישים על מהמרים

6.1.2.5.2. תכניות ניהוליות (כגון סיכומי ישיבות הנהלה, ניהול פרויקטים שוטפים,

וכיו"ב).

6.1.2.5.3. תהליכים עסקיים וממשקים עסקיים בעלי השפעה על הפעילות השוטפת והעסקית של המועצה להסדר ההימורים בספורט.

6.1.2.5.4. נתונים טכנולוגיים ו/או תפעוליים רגישים (תכניות מקצועיות הייחודיות למועצה בתחומי הטיפול והעיסוק של המועצה להסדר ההימורים בספורט וכיו"ב).

		<b>נהלי אבטחת מידע</b>
דצמבר 2017	בתוקף מ	<b>מדריך ומדיניות הגנה על המידע - טוטו</b>
מתוך 45	עמוד 22	

## 7. מערך הסיווג

7.1. מטרה: קביעת עקרונות לגבי סיווג המידע והמערכות המעבדות את המידע, על מנת להבטיח כי נכסי המועצה להסדר ההימורים בספורט יאובטחו ברמה הנדרשת.

7.2. עיקרי המדיניות:

7.2.1. ממונה אבטחת מידע יגבש קריטריונים להגדרת סיווג רגישות המידע וחיוניותו, לפי מידת הנזק שייגרם למועצה/או לגורמים אחרים, כתוצאה מחשיפה, חבלה, מחיקה או שיבוש של המידע, מאגריו או מערכותיו, בין אם במזיד ובין אם בשוגג.

7.2.2. סיווג המידע יתייחס לכל מצע או מאגר בהם קיים המידע (קבצים, בסיסי נתונים, מצעי מדיה אלקטרונית או אופטית, מסמכים, דו"חות וכדומה).

7.2.3. הסיווג יתבסס על הנזק הפוטנציאלי שעשוי להיגרם באם תיפגע רמת הסודיות, השלמות, הזמינות, הכלילות (Integrity) או השרידות של המידע או הנכס.

7.2.4. סיווגו של המידע יקבע בהתאם לרמת הרגישות הגבוהה ביותר הקיימת בקובץ, במאגר או במצע הפיזי בהם אגור המידע (על-פי עקרון "המחמיר קובע").

7.2.5. סיווג של מערכות או אפליקציות יוביל להגדרת רמת האבטחה הנדרשת, תוך התייחסות לרמת ההזדהות, רמת המידור, רמת הבקרה, צורך בהצפנה וכיו"ב. רמת האבטחה הנדרשת עבור כל מערכת תאושר על-ידי ממונה אבטחת המידע.

7.2.6. רמות הסיווג יתוו את דרכי הטיפול במידע ויתבססו על הסיכונים הפוטנציאליים הרלוונטיים למועצה והמוגדרים באופן דינאמי במסגרת ביצוע סקרי הסיכונים המתקיימים במועצה.

7.2.7. יחד עם זאת, מבוססות רמות סיווג המידע על רמת רגישותו, ומתייחסות לכל תצורה שבה נשמר המידע (אם במערכות המחשוב, אם במסמכים ואם במדיה מגנטית/אופטית).

7.2.8. סיווג המידע ייקבע על-ידי מפקח המסמך או הקובץ או על-ידי בעל המידע, במקרה של סיווג מאגרי מידע, מערכות, אפליקציות (סיווג נכסים). עובדי המועצה להסדר ההימורים בספורט יסווגו באופן עצמאי מסמכים אשר נוצרים על-ידם (כגון מסמכי Office), בהתאם להנחיות הסיווג, אשר יופצו על-ידי ממונה אבטחת מידע.

### 7.3. רמת אבטחת מידע מחייבת

7.3.1. באחריות המנכ"ל לקבוע את רמת האבטחה המחייבת את יוצרי המידע, מאגריו ומערכותיו.

7.3.2. רמת האבטחה תקיף ותכסה את המידע על כל התחומים הנגזרים ממנו (אבטחה פיזית, אבטחת רשומות, אבטחה לוגית, אבטחת מהימנות עובדים ואבטחת ממשקים עסקיים).

7.3.3. רמת אבטחת המידע בכל המערכות ומתקני המועצה להסדר ההימורים בספורט לא תהיה פחותה מרמת האבטחה המחייבת הנמוכה ביותר שתקבע.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 23	

7.3.4. כל דרישה לחריגה מרמה זו תובא מנומקת לאישור מראש של המנכ"ל.

		<b>נהלי אבטחת מידע</b>
דצמבר 2017	בתוקף מ	<b>מדריך ומדיניות הגנה על המידע - טוטו</b>
מתוך 45	עמוד 24	

## **8. אבטחת משאבי אנוש**

מטרת פרק זה הינה לקבוע עקרונות אבטחת מידע בכל הקשור לעובדי המועצה להסדר ההימורים בספורט, על מנת לצמצם את הסיכונים הנובעים מחוסר מודעות של עובדים, טעויות אנוש, התנערות מאחריות או רצון מכוון של עובד לפגוע במידע האגור במערכות המועצה להסדר ההימורים בספורט.

### 8.1 . אבטחת מידע בתהליכי גיוס וגרירת עובדים

8.1.1 **מטרה:** צמצום את סיכוני אבטחת המידע, הנובעים מגיוס עובדים בעלי רמה נמוכה של מהימנות ומחויבות אישית, וצמצום הסיכונים הכרוכים בעזיבת עובדים.

#### 8.1.2 . עיקרי המדיניות:

8.1.2.1 ראיונות ראשוניים בארגון יבוצעו על ידי אנשי התפקידים הרלוונטיים, כפי שיקבע במסמך המפרט את תהליך הגיוס בהתחשב/בהתאם לאופי המשרה.

8.1.2.2 סמנכ"ל משאבי אנוש במועצה להסדר ההימורים בספורט יבצע בדיקות ברשתות החברתיות על המועמדים.

8.1.2.3 החוזה שנחתם עם עובדים חדשים יכלול התייחסות לאחריות של העובד בכל הנוגע להיבטי אבטחת מידע, וילווה בהצהרת סודיות, אשר עליה יהיו מחויבים לחתום כל עובדי המועצה להסדר ההימורים בספורט.

8.1.2.4 עובדים העוזבים את המועצה להסדר ההימורים בספורט יחזירו למועצה את כל המידע וכן את כל ציוד המחשוב (חומרה ותוכנה) הנמצא ברשותם, ובכלל זה מוצרי אבטחת מידע (כגון כרטיס להתחברות מרחוק לרשת, מחשב נייד).

8.1.2.5 הרשאות העובדים במערכות המועצה להסדר ההימורים בספורט יבוטלו מיד עם עזיבת העובד.

8.1.2.6 ממונה אבטחת מידע במועצה להסדר ההימורים בספורט יגדיר את הגורמים הרשאים לגשת לקבצים שהיו בבעלות העובד העוזב.

### 8.2 . עקרון האחריות האישית

8.2.1 **מטרה:** להבטיח את מחויבות העובדים לאבטחת המידע המצוי ברשותם.

#### 8.2.2 . עיקרי המדיניות:

8.2.2.1 כל עובד במועצה יהיה אחראי באופן אישי לאבטחת המידע אליו הוא נחשף במהלך עבודתו ולכלל המידע המצוי בחזקתו, לרבות כזה אשר נשלח או הועבר אליו על-ידי גורם אחר. כל פגיעה במידע שתנבע מרשלנות של העובד או מאי עמידה בנהלים תהיה באחריות העובד.

8.2.2.2 הנהלת המועצה להסדר ההימורים בספורט מצפה מכל עובד לראות עצמו כאחראי ולפעול לדווח ישירות ומיד או לממונה אבטחת מידע, על כל פעילות העלולה להשפיע על אבטחת המידע.

8.2.2.3 האחריות לאבטחת המידע, בין אם הנה מוטלת על עובדי המועצה להסדר ההימורים בספורט ובין אם על מנהליו, מתייחסת לאבטחה הפיזית, אבטחת הרשומות והאבטחה הלוגית.



		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 25	

8.2.2.4. במסגרת אחריות זו, על העובד לנקוט בכל האמצעים העומדים לרשותו על מנת להגן על המידע. בין אמצעים אלה:

8.2.2.4.1. שימוש אישי בזיהוי המשתמש.

8.2.2.4.2. שמירה על חיסיון הסיסמא.

8.2.2.4.3. דיווח על חריגות אבטחת מידע.

8.2.2.4.4. שמירה מאובטחת של מסמכים ורשומות.

8.2.2.4.5. אבטחת סביבת העבודה.

8.2.2.5. עקרון האחריות האישית יוטמע במועצה בעזרת האמצעים הבאים:

8.2.2.5.1. החתמת העובדים על הצהרת סודיות ואחריות.

8.2.2.5.2. העלאת מודעות העובדים לנושאי אבטחת מידע באמצעות הדרכות והפצת חוזרים בנושא.

8.2.2.5.3. טיפול משמעותי באירועי אבטחת מידע.

8.2.2.5.4. שימוש בכלים טכניים, המאפשרים בקרה על יישום האחריות האישית (כגון: הגדרת חשבונות אישיים בלבד בכל המערכות ויישום כלי בקרה).

### 8.3. הדרכות אבטחת מידע

8.3.1. מטרה: להבטיח כי עובדי המועצה להסדר ההימורים בספורט מודעים לסיכונים בכל הקשור לאבטחת מידע ובידם הכלים ליישום מדיניות ונהלי אבטחת המידע של המועצה להסדר ההימורים בספורט.

8.3.2. עיקרי המדיניות:

8.3.2.1. כל עובדי המועצה להסדר ההימורים בספורט יחויבו להשתתף בהדרכות אבטחת מידע בהתאם למידת הידע הנחוץ לכל בעל תפקיד. ממונה אבטחת מידע יגדיר תכנית הדרכה מפורטת, אשר בה יפורטו תכני ההדרכות ותדירותן עבור עובדי המועצה להסדר ההימורים בספורט.

8.3.2.2. בנוסף להדרכות תקופתיות, כל עובד חדש יעבור הדרכה בנושאי אבטחת מידע במסגרת ההכשרה הראשונית בחברה.

8.3.2.3. בנוסף להדרכות הפרונטאליות, יופצו על-ידי ממונה אבטחת מידע חוזרים שוטפים בנושאי אבטחת מידע, כולל עדכונים על אירועי אבטחת מידע שאירעו במועצה ומחוצה לה להעלאת המודעות לאבטחת מידע בקרב עובדי המועצה להסדר ההימורים בספורט, ממשקיה והגורמים האחריים להם נגישות למידע.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 26	

## 9. נהלים

9.1.1. מטרה: לתעד ולעגן תהליכי עבודה אחידים שיחייבו את כל גורמי המקצוע והעובדים הרלוונטיים, בכל היבטי אבטחת המידע.

9.1.2. עיקרי המדיניות:

9.1.2.1. ממונה אבטחת מידע אחראי לפיתוח נהלים לשם הסדרת פעילויות אבטחת המידע בחברה.

9.1.2.2. נוהלי אבטחת המידע חלים על כל עובדי המועצה להסדר ההימורים בספורט ועל ממשקיו באשר הם, אשר להם מעורבות בפיתוח, בתפעול, בתחזוקה, ביישום ובשימוש במידע.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 27	

## 10. טיפול באירועי אבטחת מידע

10.1.1. מטרה: לקבוע עקרונות דיווח וטיפול באירועי אבטחת מידע, באמצעותם ניתן יהיה לצמצם את הנזק שיגרם כתוצאה מהאירועים, לתקן את הליקויים, לטפל משמעתית בגורמים הרלוונטיים ולהפיק לקחים לעתיד.

10.1.2. עיקרי המדיניות:

10.1.2.1. על כל עובד במועצה לדווח על אירועים / בעיות / חשדות לבעיות אבטחת מידע בהם הוא נתקל במהלך עבודתו.

10.1.2.2. ממונה אבטחת מידע ירכז את הטיפול באירועי אבטחת מידע הנושאים סיכון נמוך עד בינוני עבור המועצה. ממונה אבטחת מידע ירכז את הטיפול באירועי אבטחת מידע בעלי סיכון גבוה עבור המועצה להסדר ההימורים בספורט (אירועים אשר יש בהם משום פגיעה קשה במאזן הכספי של המועצה להסדר ההימורים בספורט, פגיעה קשה בתפעולה או בתדמיתה).

10.1.2.3. חריגות בתחום אבטחת המידע המאותרות על-ידי גורמי המועצה להסדר ההימורים בספורט או אחרים, ידווחו לממונה אבטחת מידע ויועברו לפי הצורך להמשך טיפול לגורם הרלוונטי בחברה.

10.1.2.4. לכל פעילות חריגה בעלת השלכות על אבטחת המידע יוגדר אופן רישומה, הדיווח עליה ואופן התגובה הנדרש.

10.1.2.5. הטיפול באירועי אבטחה יכלול תחקיר של האירוע, תיקון הליקויים (כולל סגירת הפרצות ברמה הטכנית והנוהלית) והפקת לקחים לעתיד.

10.1.2.6. במקרה הצורך בקיומו של טיפול משמעותי בעקבות אירוע אבטחת מידע, ייקבע הטיפול לחומרת העבירה וינוע מנזיפה על-ידי דרגי ההנהלה השונים ועד לפיטורין ו/או פניה למשטרה.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 28	

## 11. שימוש בציווד המחשוב במועצה

11.1.1. מטרה: צמצום הסיכונים הנובעים משימוש לא מורשה בציווד המחשוב במועצה בכלל, ובמחשבים האישיים והניידים בפרט.

11.1.2. עיקרי המדיניות:

11.1.2.1. ממונה אבטחת מידע, יגדיר את ההנחיות לשימוש מאובטח בציווד על-ידי עובדי המועצה להסדר ההימורים בספורט.

11.1.2.2. ההנחיות יופצו לעובדי המועצה להסדר ההימורים בספורט בהתאם לרלוונטיות, לרבות הפצתן של הוראות הפעלה טכניות של מערכות לוגיות או פיזיות, רכיבי או מנגנוני אבטחה, מחשבים ניידים וכיו"ב.

11.1.2.3. ממונה אבטחת מידע יודא יישום נאות של ההנחיות על-ידי העובדים וכן שימוש הולם ומאובטח בציווד.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 29	

## 12. אבטחת מידע בעבודה מול ספקים חיצוניים ובעלי העניין

12.1.1. מטרה: צמצום הסיכונים הנובעים מחשיפה של עובדי חברות חיצוניות למידע ולמערכות של חברה.

12.1.2. עיקרי המדיניות:

12.1.2.1. הממשקים העסקיים נבדלים זה מזה בהיקף ואופן חשיפתם למידע המצוי בחברה. חלקם של ממשקים אלו חשופים לגורמים חיצוניים.

12.1.2.2. ממונה אבטחת מידע יתווה תהליכים ושיטות טיפול אבטחתי בממשקים עסקיים, לרבות:

- קריטריונים להגדרת רגישות / סיווג הממשק העסקי.
- דרישות אבטחתיות בכפוף לסיווג הממשק העסקי.
- שיטות וכלים לאכיפת הדרישות.
- תהליכים ואמצעים לפיקוח ובקרה ולטיפול בחריגים.

12.1.2.3. כל התקשרות של המועצה להסדר ההימורים בספורט עם צד שלישי, לכל צורך שהוא הכרוך בחשיפה של עובדי הספק למידע של המועצה להסדר ההימורים בספורט (יהיו אלה יועצים, עובדים חיצוניים קבועים, ספקי תמיכה טכנית וכו'), תתבסס על חוזה בין הצדדים, הכולל התייחסות לאחריות של הספק בכל הנוגע להיבטי אבטחת מידע.

12.1.2.4. ניסוח פרק אבטחת המידע בחוזה יתבצע על-ידי גורמי אבטחת המידע בסיוע של גורמי הרכש.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 30	

- 12.1.2.5. המועצה להסדר ההימורים בספורט מחויבת לשמירת המידע הארגוני המשמש אותה בתהליכי מתן השירותים של לקוחותיה ובכלל זה מידע על חוזים, ומידע פנימי של לקוחותיה.
- 12.1.2.6. לקוחותיה וספקיה של חברת המועצה להסדר ההימורים בספורט מחויבים בחתימה על מסמך הסכם סודיות
- 12.1.2.7. המועצה להסדר ההימורים בספורט תפעל בשיתוף פעולה עם בעלי העניין, בכל ההיבטים הנוגעים לאבטחת המידע.
- 12.1.2.8. השמירה על אבטחת המידע היא מעניינו ובאחריותו של כל אחד מהמנהלים ועובדי המועצה וספקיה וביניהם קבלי המשנה.
- 12.1.2.9. הנהלת המועצה להסדר ההימורים בספורט תביא לידיעת כלל העובדים, הקבלנים, הספקים ובעלי העניין את מדיניות המועצה בתחום אבטחת המידע במטרה להבטיח את מודעותם להתחייבויות שלהם ואליהם בתחום אבטחת המידע.
- 12.1.2.10. ניסוח פרק אבטחת המידע בחוזה יתבצע על-ידי גורמי אבטחת המידע בסיוע של גורמי הרכש.

		<b>נהלי אבטחת מידע</b>
דצמבר 2017	בתוקף מ	<b>מדריך ומדיניות הגנה על המידע - טוטו</b>
מתוך 45	עמוד 31	

### 13. אבטחה פיזית

#### 13.1. בקרת גישה

13.1.1. **מטרה:** הגנה על מכלול הציוד והמידע המצויים באתר המועצה להסדר ההימורים בספורט מפני גישה פיזית של גורמים בלתי מורשים, אשר תוצאותיה עשויות להיות חשיפה, גניבה, שינוי או הרס של מידע.

13.1.2. עיקרי המדיניות:

13.1.2.1. מדיניות האבטחה בחברה, כתפיסה כללית, אמורה להיות מורכבת ממספר "מעגלי אבטחה", אשר במרכזם ניצבים נכסייה היקרים של המועצה להסדר ההימורים בספורט, אותם הוגדר שיש צורך לאבטח, לרבות מידע, האמור להיתפס כאחד מן הנכסים העיקריים והמהותיים ביותר בחברה.

13.1.2.2. האזורים הרגישים ייקבעו על-ידי ממונה אבטחת מידע.

13.1.2.3. ממונה אבטחת מידע יקבע מדיניות הרשאות גישה לרכיבי המערכת השונים, לרבות מחשבים וציוד תקשורת וכן את דרכי האכיפה והבקרה על ביצוען.

#### 13.2. אבטחת סביבת העבודה

13.2.1. **מטרה:** הגנה על המידע המצוי בסביבת העבודה האישית של כל עובד מפני גישה פיזית של גורמים בלתי מורשים, אשר תוצאותיה עשויות להיות חשיפה, גניבה, שינוי או הרס של המידע.

13.2.2. עיקרי המדיניות:

13.2.2.1. כל עובד אחראי לאבטחת סביבת העבודה האישית שלו. אבטחת סביבת העבודה תתבסס על שני עקרונות מרכזיים:

13.2.2.2. מדיניות "שולחן נקי" (Clear desk policy):

13.2.2.3. מצעים פיזיים נושאי מידע (מסמכים, דיסקים, דיסקטים וכיו"ב) בסיווג "חסוי ביותר", לא יותרו חשופים על השולחן כאשר עוזב העובד את סביבת העבודה בסופו של יום העבודה.

13.2.2.4. מדיניות "מסך נקי" (Clear screen policy):

- אין להותיר את המחשב פתוח (במצב של חיבור לרשת) כאשר עוזבים את סביבת העבודה.

- במהלך יום העבודה ואין להשאיר אמצעי הזדהות ללא השגחה.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 32	

## 14. אבטחת רשומות

14.1. מטרה: הגדרת תהליכי וכלי הטיפול ברשומות (מצעים פיזיים נושאי מידע), במטרה לצמצם את סיכוני הפגיעה במידע האגור בהם.

14.2. עיקרי המדיניות:

14.2.1. רשומות מידע כוללות מצעי מידע פיזיים כגון מסמכים, תדפיסים, דיסקים, קלטות וסרטים.

14.2.2. קיומו של מידע רגיש על-גבי מצעים פיזיים אשר הגעתם לידיים עוינות עלולה להוביל לנזקים. סיכוני אבטחת המידע קיימים לרשומות הנמצאות בשטח העבודה, מידע ברשומות עשוי לעתים להימצא מחוץ לשטח העבודה (לצרכי ישיבות או עבודה מרחוק וכן משום השלכת מסמכים לפחי אשפה הנלקחים מחוץ לבניין), שם הנו חשוף לסיכונים נוספים.

14.2.3. ממונה אבטחת מידע יגדיר את אמצעי ותהליכי הטיפול באבטחת רשומות, בהתאם לרגישות המידע. תחומי ההתייחסות יכללו:

14.2.3.1. שיטות וכלים לאבטחת מידע והשמדתו, בהתאם לסיווג המידע.

14.2.3.2. תהליכי ואמצעי שינוע מידע (פנים וחוץ ארגוני).

14.2.3.3. טיפול בחריגים.

14.2.3.4. אופן ביצוע פיקוח ובקרה.



		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 33	

## 15. אבטחה לוגית

### 15.1. שכבות האבטחה הלוגית :

15.1.1. **מטרה:** הגדרת שכבות האבטחה בתחומים הלוגיים, המהווים מעגלי הגנה על המידע, בתחומי המחשוב והתקשורת.

15.1.2. עיקרי המדיניות :

15.1.2.1. האבטחה הלוגית מהווה את ה"שכבה" העיקרית והקרובה ביותר בהגנה על המידע המצוי במערכות המחשב והתקשורת.

15.1.2.2. העדר יישום נכון של "שכבה" זו, חושף את המידע לפעילויות שונות, אשר חלקן עלולות להסב נזק רב לחברה.

15.1.2.3. ממונה אבטחת המידע יתווה את רמת האבטחה הלוגית המחייבת עבור רכיביהן השונים של מערכות המחשוב והתקשורת.

15.1.2.4. תיושם הגנה לוגית במערכות ההפעלה, בתוכנות ובאפליקציות, בקבצי ובבסיסי נתונים, בפעולות שינוי של הנתונים (ברמת הרשומה, השדות וסוג הפעולה) ובתקשורת.

15.1.2.5. תחומי התייחסות של ממונה אבטחת מידע בהיבטים הלוגיים יכללו התוויה, הגדרה ובקרת יישום של:

- שיטות וכלים לאבטחת מידע במערכות המחשב והתקשורת, בהתאם לסביבות העבודה ולהגדרות הפרופילים שיקבעו.
- טיפול בחריגים.
- אופן ביצוע פיקוח ובקרה.

### 15.2. איסור שינוי לא מבוקר :

15.2.1. **מטרה:** צמצום נזקים למידע ולמערכות העלולים לנבוע משינויים בלתי מבוקרים, העלולים להשפיע על תפעול המערכות והתהליכים.

15.2.2. עיקרי המדיניות :

15.2.2.1. יוגדרו נהלים המתווים את אופן ביצוע השינויים בנתונים, בתוכנות יישומיות, בתוכנות תשתית ובחומרה של מערכות המועצה להסדר ההימורים בספורט.

15.2.2.2. חל איסור על ביצוע שינוי בנתונים שלא במהלך הפעילות הרגילה, בתוכנה יישומית, בתוכנת תשתית ובחומרה, אלא אם הדבר נעשה באופן מאובטח ומבוקר ובהתאם להנחיות ממונה אבטחת המידע, תוך התייעצות עם גורמי ההנהלה הרלוונטיים.

15.2.2.3. ממונה אבטחת מידע יוכל לאשר שינויים בהתאם לצורך.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 34	

### 15.3. בקרת שינויים:

15.3.1. **מטרה:** להבטיח כי לא תיווצרנה פרצות אבטחת מידע במערכות המועצה להסדר ההימורים בספורט כתוצאה מביצוע שינויים במערך המחשוב.

#### 15.3.2. עיקרי המדיניות:

15.3.2.1. לא יבוצעו שינויים במערך המחשוב והתקשורת, אשר יש להם השפעה על אבטחת המידע בחברה, ללא אישור גורמי אבטחת המידע.

15.3.2.2. סוגי שינויים אפשריים:

- שינוי במבנה ובפריסה של הרשת.
  - שינוי חומרה או תוכנה במערכות המועצה להסדר ההימורים בספורט (כולל עדכון גרסאות).
  - שינוי הגדרות במערכות.
  - שינוי בנוהלי העבודה.
- 15.3.2.3. השינויים המתוכננים יאושרו על-ידי ועדת ההיגוי במסגרת אישור תכנית העבודה השנתית, ויתבצעו בהתאם לנהלים ולהנחיות אשר יוגדרו על-ידי ממונה אבטחת מידע.
- 15.3.2.4. שינויים שלא יאושרו במסגרת תכנית העבודה, או שיהיו חריגה מנהלי המועצה להסדר ההימורים בספורט, יעברו את המסלול שלהלן:

- תיעוד הבקשה לשינוי על-ידי יוזם השינוי, והעברת הבקשה לנאמן אבטחת המידע.
- הערכת ההשלכות האבטחתיות של השינוי על-ידי ממונה אבטחת מידע.
- במקרים של צורך בשינויים בחירום, לא יהיה צורך ביישום המסלול הנ"ל, והשינוי ידווח בדיעבד אך בהקדם האפשרי, לממונה אבטחת מידע.

### 15.4. הפרדת סמכויות

15.4.1. **מטרה:** צמצום אפשרויות הפגיעה במידע על ידי אדם אחד, אם מתוך כוונת זדון ואם שלא במתכוון.

#### 15.4.2. עיקרי המדיניות:

- 15.4.2.1. בתהליכים רגישים בחברה, ובפרט בתהליכים אשר יש בהם פוטנציאל לביצוע מעילות או הונאות או גנבת ידע יש ליישם הפרדת סמכויות.
- 15.4.2.2. משמעות הפרדת הסמכויות היא כי אדם אחד לא יוכל לבצע לבדו תהליך מלא. לדוגמא: אדם אחד לא יוכל הן ליזום הזמנה וגם לאשרה.
- 15.4.2.3. לצורך מימוש עקרון זה, על מערכות המחשוב השונות לתמוך בהפרדת

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 35	

הסמכויות המוגדרת בחברה. מערכות ההרשאות יימנעו ממשתמשים לבצע פעולות המוגדרות כמופרדות זו מזו.

15.4.2.4. תהליך האפיון והיישום של הפרדת הסמכויות במועצה יונחה על-ידי מנכ"ל המועצה להסדר ההימורים בספורט.

### 15.5 ניהול רשת התקשורת

15.5.1. מטרה: קביעת עקרונות לניהול מאובטח של מערך התקשורת של המועצה להסדר ההימורים בספורט, לצורך צמצום הסיכונים הנובעים מקישור בתקשורת בין מערכות המועצה להסדר ההימורים בספורט ובין לעולם החיצון.

15.5.2. עיקרי המדיניות:

15.5.2.1. גישה לתוך המועצה לגורמים וספקים חיצוניים תינתן הגישה תיפתח אך ורק על גבי תשתית SSL VPN. כל גישה ופעילות של ספק חיצוני תוקלט ע"י מערכת הסייברארק.

15.5.2.2. הקריטריונים למתן הרשאות להתחברות בתקשורת מ/אל רשת המועצה להסדר ההימורים בספורט יוגדרו על-ידי ממונה אבטחת מידע הפרמטרים שיוגדרו:

- מי מורשה להתחבר.
- טווחי הזמנים בהם מותרת ההתקשורת - באילו ימים (האם כולל סופי שבוע) ובאילו שעות של היום.
- הפעילויות המותרות - רמת ההרשאות במערכות ושימוש בשרותי התקשורת השונים.
- רמת ההזדהות הנדרשת.

15.5.2.3. ייושם מידור בין החלקים השונים ברשת באמצעות חלוקת הרשת לסגמנטים והגבלת אפשרות הקישור בין הסגמנטים השונים. רמת המידור תיקבע בהתאם לרמת הרגישות של המערכות.

15.5.2.4. תיושם הגנה על ציוד התקשורת. ההגנה תיושם ברמה הפיזית (נעילת ארונות/חדרי תקשורת, הגבלת גישה) וברמה הלוגית (הגבלה מקסימאלית של התחנות והגורמים המורשים לבצע שינויים, יישום מערך סיסמאות חזק וכו').

### 15.6 הרשאות גישה

15.6.1. מטרה: הגבלת הגישה של עובדים למידע האגור במערכות המועצה להסדר ההימורים בספורט לצורך צמצום אפשרויות הפגיעה במידע על ידי העובדים עצמם או על ידי גורמים חיצוניים, ששיגו גישה בלתי מורשית למערכות.

15.6.2. עיקרי המדיניות:

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 36	

15.6.2.1. הרשאות הגישה במועצה ייושמו ברמות הבאות :

- ברמת האפליקציה.

- ברמת הרשת

15.6.2.2. יבוצע מידור של המידע ושל המשתמשים בו. ההרשאות יינתנו על בסיס

"פרופילי הרשאות". לכל בעל תפקיד במועצה יוגדר פרופיל הרשאות מתאים לו יוענקו הרשאות גישה לפרטי מידע הדרושים לו לביצוע עבודתו בלבד, כפי שיוגדר על ידי ממונה אבטחת מידע בשיתוף בעלי המידע.

15.6.2.3. מידור המידע יעשה על ידי חלוקת המידע והמשתמשים לקבוצות שייכות או

עניין ובהתאם לסביבות העבודה (פרופילי משתמשים).

15.6.2.4. המידור יתבצע בהתאם לעקרון "הצורך לדעת", המצמצם במידת האפשר את

הגורמים המורשים להיחשף לנכסי המידע הרגישים במיוחד, ומאפשר שקיפות בתוך המועצה להסדר ההימורים בספורט ביחס לנכסי מידע בסיווג נמוך יותר.

15.6.2.5. עקרונות המידור יוגדרו על-ידי ממונה אבטחת מידע והגורמים המקצועיים

בכל תחום פעילות בחברה.

15.6.2.6. חריגות מפרופילי ההרשאות, או בקשות למתן הרשאות למידע, אשר אינן

נכללות במסגרת הפרופילים המוגדרים, יאושרו על-ידי בעל המידע הרלוונטי.

#### 15.7. בקרה על ביצוע פעולות לא מורשות

15.7.1. מטרה : איתור ניסיונות מוצלחים או כושלים לביצוע פעולות לא מורשות במערכות

המועצה להסדר ההימורים בספורט.

15.7.2. עיקרי המדיניות :

15.7.2.1. איתור הניסיונות לביצוע פעולות לא מורשות ברשת המועצה להסדר ההימורים

בספורט יתמקד בניתוח בדיעבד של מנגנוני הבקרה (הלוגים) במערכות ובמוצרי האבטחה השונים. הבקרה הסטנדרטית תתמקד באיתור ניסיונות כניסה כושלים למערכת/לרשת ופעילות בשעות חריגות. במערכות רגישות יבוצעו פעילויות בקרה ברמה גבוהה יותר כדוגמת מעקב אחר חשבונות פריבילגיים ומעקב אחר ביצוע פעולות מסוימות כגון הפקת דו"ח מהמרים. עבור כל מערכת תוגדר רמת האבטחה הנדרשת, כאשר ההגדרה תכלול הן את סוגי האירועים הנבדקים והן את הנתונים הנשמרים לגבי כל אירוע.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 37	

## 16. פיתוח ורכש

### 16.1. שילוב אבטחת מידע בתהליכי פיתוח ורכש

16.1.1. מטרה: לקבוע עקרונות לשילוב אבטחת מידע בתהליכי הפיתוח והרכש, על מנת להבטיח כי ייושמו במערכות המועצה להסדר ההימורים בספורט אמצעי אבטחה מתאימים בהתאם לרמת הרגישות של כל מערכת.

16.1.2. עיקרי המדיניות:

16.1.2.1. ממונה אבטחת המידע אחראי להגדרת דרישות אבטחת מידע, במידת הצורך, בנושאים שבפיתוח ובתחזוקה.

### 16.2. שילוב מוצרי אבטחת מידע

16.2.1. מטרה: לקבוע עקרונות לשילוב מוצרי אבטחת מידע במערכות המועצה להסדר ההימורים בספורט, על מנת להגיע לרמת אבטחת המידע הנדרשת במערכות השונות.

16.2.2. עיקרי המדיניות:

16.2.2.1. יעשה שימוש במוצרי אבטחת מידע הקיימים בשוק על מנת ליישם את רמת האבטחה הנדרשת במערכות השונות.

16.2.2.2. הצורך במוצר אבטחת מידע יקבע על בסיס שקלול שני פרמטרים: רמת הרגישות של המערכת והיכולת ליישם את רמת האבטחה הנדרשת בעזרת האמצעים המובנים במערכת עצמה.

16.2.2.3. תהליך השילוב של מוצרי אבטחת מידע:

- הגדרת הדרישות על-ידי ממונה אבטחת המידע ואיתור המוצרים העונים על הדרישות.
- בחינה טכנית של המוצרים על-ידי ממונה אבטחת מידע, בשיתוף בעל המידע, נאמן אבטחת המידע ובסיוע הגורמים הטכניים המתאימים.
- תפעול שוטף של מוצרי האבטחה על-ידי מערכות המידע.

### 16.3. שילוב מנגנוני הצפנה

16.3.1. מטרה: לקבוע עקרונות לשילוב מנגנוני הצפנה במערכות המועצה להסדר ההימורים בספורט, על מנת להגן על מידע רגיש מפני חשיפה ושינוי.

16.3.2. עיקרי המדיניות:

- 16.3.2.1. המועצה להסדר ההימורים בספורט תיישם מנגנוני הצפנה במקרים הבאים:
- הצפנת התקשורת בשירותי תקשורת רגישים, כגון גישה מרחוק לרשת, ממשקים חיצוניים

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 38	

16.3.2.2. יישום מנגנוני ההצפנה יעשה בהתאם לאילוצים הטכנולוגיים של מערכות המועצה להסדר ההימורים בספורט.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 39	

## 17. ניהול המשכיות עסקית

### 17.1. תוכנית לניהול המשכיות עסקית

17.1.1. מטרה: הגדרת העקרונות שיאפשרו את המשך הפעילות של מערכות המחשוב של מועצה בעת חירום.

17.1.2. עיקרי המדיניות:

17.1.2.1. היערכות להמשכיות עסקית נועדה לסכל הפרעות לפעילות השוטפת של המועצה להסדר ההימורים בספורט ולהגן על נתונים מפני הרס, שיבוש, מחיקה וכדומה, הנגרמים בהשפעת מקרי כשל רציניים או מקרי אסון (שריפה, הצפה, מלחמה, אסונות טבע וכדומה), במערכות המידע הפיזיות והלוגיות של המועצה להסדר ההימורים בספורט.

17.1.2.2. מנכ"ל המועצה להסדר ההימורים בספורט יגדיר דרישות, מערכות והתהליכים החיוניים להמשך פעילות המועצה להסדר ההימורים בספורט ויוגדר משך הזמן הדרוש להתאוששותם.

17.1.2.3. יזוהו האסונות והכשלים האפשריים העלולים לגרום הפרעה לפעילותו של חברה, ויוערכו השלכותיהם.

17.1.2.4. מנכ"ל המועצה להסדר ההימורים בספורט יקבע את עקרונות ההיערכות להמשכיות עסקית של מערכות המידע בחברה. באמצעות עקרונות אלו, תגובש תוכנית להתאוששות מאסון (Disaster Recovery Plan) וכן תכנית המשכיות עסקית (Business Continuity Plan), מבוססת על הערכת סיכונים נאותה המפרטת את כלל האמצעים שיש לנקוט בעקבות אירוע חירום, המסכן את הפעילות התקינה של המועצה להסדר ההימורים בספורט. התוכנית תכלול התייחסות לשלושה שלבים עיקריים בשעת חירום:

- שלב התגובה - הפעילויות המידיות שיש לנקוט בעקבות האירוע (פעולות מידיות לצמצום הנזקים, הערכת נזקי האירוע, קביעת חומרתו וכו').
- שלב ההתאוששות - הפעלת המערך החלופי בהתאם לסדר העדיפויות שנקבע.
- שלב השיקום - כלל הפעולות הנחוצות להחזרת המועצה להסדר ההימורים בספורט לשגרה שהייתה נהוגה לפני האירוע.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 40	

## 18. תכנית עבודה ותקציב

18.1. מטרה: גיבוש תכנית העבודה והתקציב בתחומי אבטחת מידע, במטרה לעמוד ביעדים ולנתב משאבים נדרשים.

18.2. עיקרי המדיניות:

18.2.1. ממונה אבטחת המידע יקיים דיוני עבודה ומעקב אחר ביצוע מדיניות אבטחת המידע.

18.2.2. ממונה אבטחת המידע ידווח תקופתית ל-מנכ"ל על פעילויות אבטחת המידע.

18.2.3. פעילות אבטחת המידע במועצה השולב בתוכנית העבודה השנתית והרב שנתית של המועצה להסדר ההימורים בספורט ותתוקצב בהתאם.



		<b>נהלי אבטחת מידע</b>
דצמבר 2017	בתוקף מ	<b>מדריך ומדיניות הגנה על המידע - טוטו</b>
מתוך 45	עמוד 41	

## 19. התאמה (COMPLIANCE)

19.1. מטרה: להבטיח כי המועצה עומדת בכל דרישות החוק הישראלי, בתקנות ובתקנים עלייהם היא מחויבת הנוגעות להיבטי אבטחת מידע.

19.2. עיקרי המדיניות:

19.2.1. באחריות מנכ"ל המועצה, לוודא כי המועצה להסדר ההימורים בספורט פועלות בהתאם לדרישות החוק הישראלי, בתקנות ובתקנים עלייהם המועצה להסדר ההימורים בספורט מחויבת.

19.2.2. המועצה להסדר ההימורים בספורט הוקמה מכוח ה"חוק להסדר ההימורים בספורט, התשכ"ז 1967".

19.2.3. להלן פירוט הוראות החוק בכל הנוגע לניהול משחקי הימורים:

19.2.4. החוק להסדר ההימורים בספורט, התשכ"ז - 1967

19.2.5. חוק הספורט, תשמ"ח 1988

19.2.6. תקנות להסדר ההימורים בספורט (תכנית הימורים בכדורגל), תשל"ח - 1978

19.2.7. תקנות להסדר ההימורים בספורט (סדרי עבודת המועצה), תשמ"ט 1989

19.2.8. תקנות להסדר ההימורים בספורט (תכנית ה"טוטו תיקון"), תש"ן 1990

19.2.9. תקנות להסדר ההימורים בספורט (תכנית הימורים יומיים) תשס"א 2001

19.2.10. תקנות להסדר ההימורים בספורט (תוכנית "סופר גול"), תשנ"ט 1999

19.2.11. בין החוקים והתקנות הרלוונטיים נוספים:

- חוק הגנת הפרטיות.
- חוק המחשבים.
- חוק זכויות יוצרים.
- חוק שירות המדינה (מינויים), תשי"ט 1959
- חוק הגנת השכר, התשי"ח 1958
- חוק שכר מינימום, התשמ"ז 1987
- חוק חופשה שנתית, התשי"א 1951

### 19.3. ביקורות אבטחת מידע

19.3.1. מטרה: הגדרת הפעילויות והכלים, אשר ישמשו את גורמי אבטחת המידע לבדיקת היישום של מדיניות אבטחת המידע, הנהלים והסטנדרטיים הטכניים במערכות השונות ובקרב

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 42	

עובדי המועצה להסדר ההימורים בספורט.

### 19.3.2. עיקרי המדיניות:

19.3.2.1. ממונה אבטחת המידע יגדיר את אמצעי ותהליכי הבקרה בתחומי אבטחת המידע של המועצה להסדר ההימורים בספורט.

19.3.2.2. באחריות המנכ"ל לבקר, בצורה שוטפת ו/או אקראית, את הפעילויות המתבצעות על / עם המידע, בכדי לוודא כי המועצה להסדר ההימורים בספורט עומדים בדרישות החוקים, התקנות, התקנים והנהלים ובהתאם לכללי המנהל התקין.

19.3.2.3. על מנת לבדוק את מידת ההתאמה בין רמת האבטחה המוגדרת לבין רמת האבטחה המיושמת בפועל, תבוצענה הפעילויות הבאות:

❖ **ביקורות טכניות:**

- לצורך בקרה על יישום מדיניות אבטחת המידע, יאפיין ויבחר ממונה אבטחת מידע כלים ייעודיים לשליטה ובקרה בתחום אבטחת המידע בשיתוף עם מנמ"ר המועצה להסדר ההימורים בספורט.
- יבוצעו ביקורות תקופתיות, לצורך בדיקת היישום הטכני של דרישות אבטחת המידע במערכות השונות, תוך שימוש בכלים ייעודיים (כלים הבודקים את הגדרות המשתמשים, הסיסמאות, ההרשאות, הגדרות המערכת וכיו"ב).
- יבוצעו מבחני חדירה (penetration tests) תקופתיים (חיצוניים ופנימיים).
- הביקורות הטכניות יוגדרו במסגרת תכנית העבודה השנתית, אשר תיכתב על-ידי ממונה אבטחת המידע ותאושר על-ידי ועדת ההיגוי.

### ❖ **ביקורות אבטחה פיזית:**

- ביצוע ביקורות מדגמיות במתחם, לבדיקת מידת היישום של נוהלי האבטחה הפיזית. תכנית הביקורות הפיזיות תוגדר על-ידי ממונה אבטחת המידע.

### ❖ **ביקורות נוהליות:**

- מנכ"ל המועצה אחראי לוודא כי עובדיו פועלים בהתאם לנוהלי אבטחת המידע של המועצה להסדר ההימורים בספורט.

### ❖ **סקר סיכונים כולל:**

- אחת לשנתיים, תבצע המועצה להסדר ההימורים בספורט סקר אבטחת מידע מקיף, אשר יכלול את בחינת יישום כלל היבטי אבטחת המידע במועצה ואתר סיכונים פוטנציאליים. סקר הסיכונים הכולל אינו מהווה תחליף לניהול הסיכונים השוטף, אשר יתבצע על-ידי ממונה אבטחת המידע. סקר הסיכונים יבוצע על-ידי גורם שלישי,

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 43	

בלתי תלוי, שאינו משולב בפעילויות האבטחה השוטפות של חברה.

		נהלי אבטחת מידע
דצמבר 2017	בתוקף מ	מדריך ומדיניות הגנה על המידע - טוטו
מתוך 45	עמוד 44	

## 20. שינוי המדיניות

### 20.1. עדכון המדיניות

20.1.1. מדיניות אבטחת המידע של המועצה להסדר ההימורים בספורט תיבדק ותאושר אחת לשנתיים, או בהתאם לצורך מיוחד (על רקע שינויים משמעותיים במערך המחשוב ו/או הארגוני של המועצה להסדר ההימורים בספורט). במקרה הצורך, תעודכן המדיניות.

20.1.2. בדיקה והעדכון יתבצעו על-ידי ממונה אבטחת המידע ויאושרו על ידי המנכ"ל.

### 20.2. חריגה מהמדיניות

20.2.1. חריגות ממדיניות זו יאושרו רק על-ידי מנכ"ל המועצה.

