



מדינת ישראל  
משרד האוצר

# נהלי סייבר חירום וביטחון

נוהל ניהול משאבי  
הגנת המידע והסייבר



## תוכן עניינים

מס'	סעיף
1	<a href="#">רקע</a>
2	<a href="#">מטרה</a>
3	<a href="#">אחריות</a>
4	<a href="#">תוקף</a>
5	<a href="#">שיטה</a>
6	<a href="#">נספחים</a>

### - פנימי -

מערך סייבר חירום וביטחון	
פרק:	כללי
מס' פרק:	5
שם הנוהל:	נוהל ניהול משאבי הגנת המידע והסייבר
מס. נוהל:	XXX
עודכן ב:	21.09.2014
ע'	Page 2 of 14

נוהל זה הינו רכושו הבלעדי של משרד האוצר. נוהל זה מצריך בדיקת עדכניות תקופתית כל 12 חודשים מיום: 25 יולי, 2017  
 לתשומת לבך- עם הדפסת הנוהל, המסמך יהפוך להיות בלתי מבוקר ותוקפו יפוג שבוע מתאריך 23 דצמבר 2019

## אישורים

תאריך	סימוכין	תפקיד	שם	מהדורה
				1.1

## שינויים בנוהל

מהות השינוי	מאשר	תאריך	מהדורה
שדרוג כל הנוהל		22/09/14	1.1

### - פנימי -

מערך סייבר חירום וביטחון	
פרק: כללי	מס' פרק: 5
שם הנוהל: נוהל ניהול משאבי הגנת המידע והסייבר	מס. נוהל: XXX
ע' Page 3 of 14	עודכן ב: 21.09.2014

## 1. מטרה

### 1.1. מטרת הנוהל

1.1.1. להגדיר את בעלי התפקידים הרלוונטיים לתחום הגנת המידע והסייבר במשרד האוצר, מטרתיהם, סמכויותיהם, תחומי אחריותם ודרישות התפקיד.

## 2. אחריות

- 2.1. מנהל תחום הגנת המידע והסייבר אחראי להתוות את מדיניות המשרד וקווי הפעולה בתחום זה.
- 2.2. אחריות יישום הנחיות נוהל זה חלה על משתמשי המחשוב עובדי המשרד ועובדי יחידות הסמך, כל אחד בתחומו, לרבות עובדי הממשקים העסקיים.
- 2.3. מנהל תחום הגנת המידע והסייבר יבקר יישום הנחיות נוהל זה.
- 2.4. אחריות עדכון נוהל זה, בהתאם לצורך, חלה על מנהל תחום הגנת המידע והסייבר.

## 3. תוקף ומסמכים

### 3.1. תוקף הנוהל

3.1.1. תוקף הנוהל-מפרסומו.

### 3.2. מסמכים מתייחסים

3.2.1. תקן ת"י ISO 27001:2013, פרק 5.3

### - פנימי -

מערך סייבר חירום וביטחון I	
פרק:	כללי
מס' פרק:	5
שם הנוהל:	נוהל ניהול משאבי הגנת המידע והסייבר
ע':	Page 4 of 14
עודכן ב:	21.09.2014

## 4. שיטה

הנהלת המשרד מסמיכה ומאצילה סמכות לבעלי התפקיד לבצע את האחריות הבאות:

### 4.1. ועדת ההיגוי לנושאי הגנת המידע והסייבר

4.1.1 מטרה: יצירת מסגרת ארגונית ניהולית לקבלת החלטות אסטרטגיות בתחום הגנת המידע והסייבר, להתעדכנות בנושאי הגנת המידע והסייבר ולביצוע בקרה ניהולית על יישום הגנת המידע והסייבר במשרד.

4.1.2 עקרונות פעילות: פורום ניהולי שמונה ע"י מנכ"ל המשרד ובראשו יושבים מנכ"ל המשרד או מי מטעמו ונועד לאשרר ולתקף את מדיניות המשרד בתחום הגנת המידע והסייבר, להתוות אסטרטגיות לפעילות, לפקח אחר תכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

4.1.3 חברי ועדת ההיגוי:

- מנכ"ל משרד האוצר
- משנה למנכ"ל משרד האוצר
- מנהל מערך סייבר חירום וביטחון
- מבקר פנים משרד האוצר
- מנהל משאבי אנוש
- מנמ"ר משרד האוצר
- נציג היועץ המשפטי
- מנהל יחידת התקצוב
- מנהל תחום הגנת המידע והסייבר

### - פנימי -

מערך סייבר חירום וביטחון	
פרק: כללי	מס' פרק: 5
שם הנוהל: נוהל ניהול משאבי הגנת המידע והסייבר	מס. נוהל: XXX
ע' Page 5 of 14	עודכן ב: 21.09.2014

במידת הצורך, ובהתאם לנושאים המתוכננים לעלות לדיון מסגרת הוועדה, יזומנו לישיבות גורמים נוספים.

#### 4.2. תפקידי ועדת ההיגוי לנושאי הגנת המידע והסייבר

- 4.2.1 התוויה של העקרונות והתפיסות הנוגעות להיבטי הגנת המידע והסייבר במשרד.
- 4.2.2 אישור מדיניות הגנת המידע והסייבר.
- 4.2.3 אישור תכנית העבודה בתחום הגנת המידע והסייבר ובקרה על יישומה.
- 4.2.4 התעדכנות בנושא אירועי הגנת מידע והסייבר חריגים שאירעו במשרד.
- 4.2.5 התעדכנות בסיכונים ובאיומים הנוגעים למשרד, פיקוח על ניהול הסיכונים המבוצע על-ידי מנהל תחום הגנת המידע והסייבר, אישור הסיכונים השיריים וקבלת החלטות באשר לצורך בביצוע שינויים בעקרונות האבטחה.
- 4.2.6 אישור רמות הסיווג של נכסי המידע.
- 4.2.7 אישור חריגות ממדיניות להגנת מידע וסייבר במשרד.
- 4.2.8 הקצאת משאבים (כסף, כ"א וזמן) ליישום דרישות תשתית הגנת המידע והסייבר.
- 4.2.9 גיבוי ניהולי של היבטי הגנת מידע וסייבר במשרד (סיוע ב"שיווק" הנושא בקרב העובדים והעלאת המודעות לתחום).

#### 4.3. דרישות התפקיד לחברי הוועדה

- 4.3.1 בהתאם לתקן 27001 אחוזי משרה משוערים (חודשי): 3%.
- 4.3.2 דרישות סף (מינימום הכרחי): מעורבות ניהולית או מקצועית בהיבטי הגנת מידע וסייבר של המשרד.
- 4.3.3 הסמכות / הכשרות: מנהל מערך סייבר חירום וביטחון - דרישה להסמכות והכשרות ניהוליות. בכל הנוגע למנהל תחום הגנת המידע והסייבר, ראה הגדרות בפרק העוסק בהם באופן ספציפי.

#### - פנימי -

מערך סייבר חירום וביטחון I	
פרק:	כללי
מס' פרק:	5
שם הנוהל:	נוהל ניהול משאבי הגנת המידע והסייבר
מס. נוהל:	XXX
עודכן ב:	21.09.2014
ע'	Page 6 of 14

#### 4.4. מנכ"ל משרד האוצר (יו"ר ועדת ההיגוי)

- 4.4.1 מטרה: להבטיח את התכנון, הניהול, הטיפול והבקרה במכלול היבטי הגנת מידע וסייבר במשרד.
- 4.4.2 עיקרי המדיניות: מנכ"ל משרד האוצר יפעל כיו"ר ועדת ההיגוי וישמש כמנהל-על לנושאי הגנת מידע וסייבר במשרד.
- 4.4.3 תפקידים וסמכויות של יו"ר ועדת ההיגוי:
- 4.4.3.1 ניהול ועדת ההיגוי לנושאי הגנת המידע והסייבר.
- 4.4.3.2 אישור מדיניות המשרד בתחומים השונים הנוגעים להגנת המידע והסייבר.

#### 4.5. מנהל מערך סייבר חירום וביטחון וממונה סייבר ארגוני

- 4.5.1 מטרה: להבטיח את התכנון, הניהול, הטיפול והבקרה במכלול היבטי הגנת מידע וסייבר במשרד.
- 4.5.2 תפקידים וסמכויות:
- 4.5.2.1 אחריות כוללת להגנת מידע וסייבר במשרד מטעם ההנהלה ובשם ועדת ההיגוי.
- 4.5.2.2 ייזום וניהול סקרי הנהלה.
- 4.5.2.3 אישור נהלי הגנת מידע וסייבר.
- 4.5.2.4 אישור תכנית הגנת מידע וסייבר, פעילויות החורגות מתוכנית ההגנה.
- 4.5.2.5 ייעוץ להנהלה ועדכונה בנושאי הגנת מידע וסייבר.
- 4.5.2.6 ייזום וניהול סקרי הנהלה בנושא הגנת מידע וסייבר.
- 4.5.2.7 גיבוש מדיניות המשרד בתחומים השונים הנוגעים להגנת מידע וסייבר.
- 4.5.2.8 בקרה אחר יישום תכנית ההגנה.
- 4.5.2.9 בקרה שוטפת והנחיית פעילותם של מנהל תחום הגנת המידע והסייבר.

#### - פנימי -

מערך סייבר חירום וביטחון I	
פרק:	כללי
מס' פרק:	5
שם הנוהל:	נוהל ניהול משאבי הגנת המידע והסייבר
מס. נוהל:	XXX
עודכן ב:	21.09.2014
ע'	Page 7 of 14

ווידוא ניהולה התקין של תכנית ניהול הסיכונים, לרבות הסיכונים השיוריים שאושרו על-ידי וועדת ההיגוי. מעורבות בטיפול באירועי הגנת המידע והסייבר בעלי סיכון גבוה למשרד.

#### 4.5.3 דרישות התפקיד:

4.5.3.1 אחוזי משרה משוערים (חודשי): 10%.

4.5.3.2 דרישות סף (מינימום הכרחי): הבנה מקצועית בסיסית בנושאי הגנת המידע והסייבר, ברמת ניהולם של התחומים (רמת "מאקרו").

4.5.3.3 הסמכות / הכשרות: הכשרה ניהולית, בהתאם לדרישות המשרד.

### 4.6. ראש תחום הגנת המידע והסייבר

4.6.1 מטרה: להטמיע ולוודא יישום היבטי הגנת מידע וסייבר הנוגעים לתחומי המחשוב והתקשורת (התחומים הלוגיים) וכן להוות גורם ניהולי מנחה לגבי צרכי האבטחה הפיזית והאנושיים הנדרשים במשרד.

#### 4.6.2 עיקרי המדיניות:

4.6.2.1 מנהל תחום הגנת המידע והסייבר יהיה כפוף ניהולית למנהל מערך סייבר חירום וביטחון.

#### 4.6.3 תפקידי מנהל תחום הגנת המידע והסייבר:

4.6.3.1 ניהול והנחייה מקצועית שוטפת בתחום הגנת מידע וסייבר.

4.6.3.2 עדכון שוטף של מנהל מערך סייבר חירום וביטחון בנוגע לנושאי הגנת המידע והסייבר.

4.6.3.3 הנחלה בשטח של החלטות וסיכומי ועדת היגוי להגנת מידע וסייבר.

4.6.3.4 הגדרת תכנית עבודה בתחומי הגנת מידע וסייבר, ניהול יישומה בשיתוף מנהל חטיבת טכנולוגיות ומיישם הגנת המידע והסייבר של יחידת מערכות מידע.

4.6.3.5 הגדרת הכלים והתהליכים הנדרשים ליישום היבטי הגנת המידע והסייבר וכן ווידוא יישומם בשיתוף מנהל חטיבת טכנולוגיות ומיישם הגנת המידע והסייבר של יחידת מערכות מידע.

#### - פנימי -

מערך סייבר חירום וביטחון I	
פרק:	כללי
מס' פרק:	5
שם הנוהל:	נוהל ניהול משאבי הגנת המידע והסייבר
מס. נוהל:	XXX
ע'י	Page 8 of 14
עודכן ב:	21.09.2014



- 4.6.3.6 גיבוש נהלים להגנת מידע וסייבר.
- 4.6.3.7 עדכון מסמך המדיניות ונהלי הגנת מידע וסייבר במשרד.
- 4.6.3.8 תכנון מטריצת רמות רגישות משרות העובדים, על-פיהן יוגדרו רמות בדיקות המהימנות הנדרשות ופרופיל הרשאות (התוכנית תאושר על-ידי ועדת ההיגוי).
- 4.6.3.9 סיוע לבעלי המידע בקביעת רמת ההגנה הנדרשת לנכסי המידע השונים של המשרד וסיוע בהטמעת יישומי הגנת המידע והסייבר, לפי הצורך (סיווג הנכסים יאושר על-ידי ועדת ההיגוי).
- 4.6.3.10 ביצוע בקרה ניהולית שוטפת אחר יישום הגנת המידע והסייבר במשרד, ובכלל זה על כל הנגזר ממסמך המדיניות, הנהלים, התקנים והחוקים המחייבים בנושאי הגנת המידע והסייבר את המשרד.
- 4.6.3.11 ווידוא יישום היבטי הגנת המידע והסייבר במערכות המשרד וכן ווידוא הטמעה ותפעול שוטף של מוצרי הגנת המידע והסייבר במערכות.
- 4.6.3.12 תיאום רכש של מוצרים או שירותים, אשר יש ברכישתם השלכות בכל הנוגע להגנת המידע והסייבר במשרד.
- 4.6.3.13 ייזום סקרי סיכונים וניהול הסיכונים במשרד.
- 4.6.3.14 ניהול ויישום תוכנית מבדקים פנימיים, אשר יבוצעו על ידו ו/או על ידי מי מטעמו.
- 4.6.3.15 טיפול בהיבטי הגנת המידע והסייבר בקרב ממשקים עסקיים.
- 4.6.3.16 הנחייה מקצועית של הגורמים העוסקים בהגנת המידע והסייבר, לפי הרלוונטיות.
- 4.6.3.17 תיאום פעילויות האבטחה בין גורמי המשרד הרלוונטיים.
- 4.6.3.18 העלאת המודעות של עובדי המשרד לנושאי הגנת המידע והסייבר.
- 4.6.3.19 התנעת הליכי טיפול משמעותי, במקרה הצורך.
- 4.6.3.20 טיפול באירועי הגנת המידע והסייבר.
- ◀ הערה: בכל הנוגע להיבטי האבטחה הפיזיים, יסתיע מנהל תחום הגנת המידע

**- פנימי -**

מערך סייבר חירום וביטחון I	
פרק:	כללי
מס' פרק:	5
שם הנוהל:	נוהל ניהול משאבי הגנת המידע והסייבר
מס. נוהל:	XXX
ע'י	Page 9 of 14
עודכן ב:	21.09.2014

והסייבר בגורמים הרלוונטיים במערך סייבר חירום וביטחון.

#### 4.6.4 דרישות התפקיד :

4.6.4.1 אחוזי משרה משוערים (חודשי) : 95%.

4.6.4.2 דרישות סף (מינימום הכרחי) : ניסיון ניהולי בדרג בינוני (ניהול צוות של שני אנשים לפחות למשך שלוש שנים, או ניהול פרויקטים חוצי ארגון במשך שלוש שנים, לכל הפחות). ניסיון טכני-מעשי בתחומי התקשורת ו/או המחשוב ו/או אבטחת המידע (שנתיים, לכל הפחות).

4.6.4.3 הסמכות / הכשרות : קורסים והסמכות מקצועיות בתחום אבטחת המידע / ה-IT (רצוי תואר אקדמי בהנדסת מערכות מידע / מדעי המחשב ו/או הסמכת CISSP ו/או הסמכת ISO27001 LEAD (AUDITOR).

### 4.7. צוותי הגנת המידע והסייבר

4.7.1 מטרה : להבטיח את יישום מדיניות הגנת מידע וסייבר במשרד, תוך פריטתה למטלות לביצוע, דרישות, הנחיות, נהלים וכלים טכנולוגיים.

4.7.2 עיקרי המדיניות :

4.7.2.1 במשרד יפעל צוות להגנת מידע וסייבר ברמה הלוגית, אשר יפעל תחת מערכות מידע.

4.7.2.2 הצוות יתכנס באופן שוטף ועל-פי הצורך בהתאם לפרויקטים, משימות אבטחה מיוחדות, אירועים חריגים וכיוצא באלו, בהתאם לשיקול דעתו של CTO ו/או מנהל תחום הגנת המידע והסייבר ו/או מנהל אגף חירום וביטחון.

4.7.3 תפקידי צוותי סייבר והגנת מידע :

4.7.3.1 סיוע בהטמעה של עקרונות המדיניות, הנהלים, הנחיות עבודה ומתודולוגיות בנושאי הגנת המידע והסייבר באגף מערכות מידע.

4.7.3.2 סיוע בהגדרת הסטנדרטים ליישום הטכני של הגנת המידע והסייבר במערכות המשרד.

#### - פנימי -

מערך סייבר חירום וביטחון I	
פרק :	כללי
מס' פרק :	5
שם הנוהל :	נוהל ניהול משאבי הגנת המידע והסייבר
מס. נוהל :	XXX
ע' :	Page 10 of 14
עודכן ב :	21.09.2014

- 4.7.3.3 סיוע בהגדרת דרישות הגנת המידע והסייבר בפיתוח ורכש של מערכות המשרד, ובקרה על יישומן במהלך הפרויקטים השונים.
- 4.7.3.4 סיוע באפיון והקמה של מערך פרופיל ההרשאות במשרד.
- 4.7.3.5 התעדכנות בטכנולוגיות הגנת המידע והסייבר ואיתור טכנולוגיות ומוצרים המתאימים למשרד.
- 4.7.3.6 תפעול שוטף של מוצרי הגנת המידע והסייבר.
- 4.7.3.7 איתור ודיווח על אירועים חריגים.
- 4.7.4 דרישות התפקיד:
- 4.7.4.1 אחוזי משרה משוערים (חודשי): 80%.
- 4.7.4.2 דרישות סף (מינימום הכרחי): ניסיון מעשי בתחומי התקשורת והמחשוב, לגבי צוות ה-IT, או בתחומי האבטחה הפיזית (שנתיים, לכל הפחות).
- 4.7.4.3 הסמכות / הכשרות: לא נדרש כדרישת סף.

#### 4.8. נאמני הגנת המידע והסייבר

- 4.8.1 מטרה: קיום נציגות הגנת המידע והסייבר ביחידות המשרד השונות, על מנת להבטיח הטמעה מיטבית של מדיניות הגנת המידע והסייבר בכלל חלקי הארגון.
- 4.8.2 עיקרי המדיניות: מנהל תחום הגנת המידע והסייבר ימנה נאמני הגנת המידע והסייבר יחידתיים בסיוע המנהלים הישירים וינחה אותם בהיבטים המקצועיים הנוגעים להגנת המידע והסייבר הרלוונטיים ליחידותיהם.
- 4.8.3 תפקידי נאמני הגנת המידע והסייבר:
- 4.8.3.1 קיום ויישום של תהליכי, שיטות וכלי הגנת המידע והסייבר, כמוגדר על-ידי מנהל תחום הגנת המידע והסייבר.
- 4.8.3.2 סיוע בגיבוש הנחיות, סטנדרטים ודרישות בכל הנוגע לאבטחת המערכות והתהליכים הנמצאים בתחום האחריות של היחידה.

#### - פנימי -

מערך סייבר חירום וביטחון I	
פרק:	כללי
מס' פרק:	5
שם הנוהל:	נוהל ניהול משאבי הגנת המידע והסייבר
מס. נוהל:	XXX
ע'י	Page 11 of 14
עודכן ב:	21.09.2014

- 4.8.3.3 סיוע בבקרה על היישום התפעולי של הנחיות הגנת המידע והסייבר.
- 4.8.3.4 סיוע בניהול הבחינה הטכנית וההטמעה של טכנולוגיות ומוצרי הגנת המידע והסייבר.
- 4.8.3.5 סיוע בהגדרת דרישות הגנת המידע והסייבר בפיתוח ורכש של מערכות חדשות עבור היחידה.
- 4.8.3.6 סיוע בתיאום פעילויות הגנת המידע והסייבר ביחידה.
- 4.8.3.7 דיווח על ליקויי הגנת המידע והסייבר ועל אירועים חריגים ביחידה.
- 4.8.3.8 העלאת מודעות עובדי היחידה לנושאי הגנת המידע והסייבר.
- 4.8.3.9 סיוע בהעברת מידע ומסרים לעובדי היחידה בנושאי הגנת המידע והסייבר.
- 4.8.3.10 ביצוע ביקורות תקופתיות בנושאים שייקבעו על-ידי מנהל תחום הגנת המידע והסייבר ו/או מנהל אגף חירום וביטחון.
- 4.8.3.11 ייזום דרישות לפעילויות הגנת המידע והסייבר בתחומים הנוגעים ליחידה.
- 4.8.4 דרישות התפקיד:
- 4.8.4.1 אחוזי משרה משוערים (חודשי): 5%.
- 4.8.4.2 דרישות סף (מינימום הכרחי): הבנה בסיסית בנושאי הגנת המידע והסייבר (לכל הפחות, ברמת הסיכונים הפוטנציאליים). העסקה של לפחות שנה במשרד, בדרג ניהולי בינוני ומעלה. בעל אחריות ולויאליות למשרד. בעל אסרטיביות ומנהיגות. יכולת דיווח, סדר וארגון.
- 4.8.4.3 הסמכות / הכשרות: הדרכות ורענונים שיועברו על-ידי מנהל תחום הגנת המידע והסייבר, בשיתוף יחידת ההדרכה של משרד האוצר.
- 4.8.4.4 הערה: המפורט בסעיף זה מתייחס לכל נאמני הגנת המידע והסייבר, בכל האגפים, באופן זהה ואחיד (אין דרישות ייחודיות הנגזרות מהעסקתו של נאמן ביחידה מסוימת).

**- פנימי -**

מערך סייבר חירום וביטחון I	
פרק:	כללי
מס' פרק:	5
שם הנוהל:	נוהל ניהול משאבי הגנת המידע והסייבר
מס. נוהל:	XXX
ע'י	Page 12 of 14
עודכן ב:	21.09.2014

**4.9. בעלי מידע**

4.9.1 מטרה: קביעת אחראי לכל אחד מנכסי המידע במשרד, על מנת להבטיח כי כל נכסי המידע יאובטחו ברמה הנדרשת.

4.9.2 עיקרי המדיניות: לכל סוג מידע במשרד (בהתאם למערכות ולמאגרי המידע השונים) יקבעו בעלים. בעלי המידע יהיו גורמים ניהוליים במשרד, המהווים את המשתמשים העיקריים בכל נכס מידע. בעלי המידע ימונו על-ידי מנכ"ל המשרד, בסיוע המנהלים הישירים.

4.9.3 תפקידי בעלי המידע:

4.9.3.1 קביעת סיווגו של נכס המידע.

4.9.3.2 קביעת הגורמים המורשים לגשת למידע ואישור בקשות לחריגות מרשימה זו.

4.9.3.3 ייזום דרישות הגנת המידע והסייבר והעברתן למנהל תחום הגנת המידע והסייבר.

4.9.3.4 דיווח למנהל תחום הגנת המידע והסייבר על כל אירוע חריג הנוגע למידע שבבעלותו.

4.9.3.5 הערה: במאגרים המכילים מידע הנוגע לצנעת הפרט, בעל המידע ישמש גם כ"מנהל מאגר המידע" (בהתאם לדרישות חוק הגנת הפרטיות).

4.9.4 דרישות התפקיד:

4.9.4.1 אחוזי משרה משוערים (חודשי): 2%.

4.9.4.2 דרישות סף (מינימום הכרחי): הבנה בסיסית בנושאי הגנת המידע והסייבר (לכל הפחות, ברמת הסיכונים הפוטנציאליים). העסקה של לפחות שנה במשרד.

4.9.4.3 הסמכות / הכשרות: הדרכות ורענונים שיועברו על-ידי מנהל תחום הגנת המידע והסייבר ו/או סגן מנהל אגף חירום וביטחון.

**- פנימי -**

מערך סייבר חירום וביטחון I	
פרק:	כללי
מס' פרק:	5
שם הנוהל:	נוהל ניהול משאבי הגנת המידע והסייבר
מס. נוהל:	XXX
ע'י	Page 13 of 14
עודכן ב:	21.09.2014

**4.10. מנהלים**

4.10.1 מטרה: לקבוע את מחויבות המנהלים בדרגות השונות, להיבטי הגנת המידע והסייבר אשר נוגעים לתחומי עיסוקם.

4.10.2 עיקרי המדיניות:

באחריות כל מנהל במשרד:

4.10.2.1 לוודא יישום של מדיניות ונהלי הגנת המידע והסייבר של המשרד בקרב עובדיו.

4.10.2.2 לעדכן את מנהל תחום הגנת המידע והסייבר אודות כוונה לבצע רכש של מוצרים או שירותים, לרבות בנסיבות של שדרוג, תחזוקה או החלפת ספקים. כל זאת, על-מנת לאפשר למנהל תחום הגנת המידע והסייבר לשקול את הצורך בשילוב היבטי אבטחה.

4.10.2.3 להעלות את מודעות עובדי היחידה לנושאי הגנת המידע והסייבר.

4.10.2.4 לדווח למנהל תחום הגנת המידע והסייבר אודות תקלות, כשלים או סיכונים הנוגעים לפעילות היחידה או לתפקוד עובדיו.

4.10.2.5 לספק את הסיוע הנדרש לגורמי הגנת המידע והסייבר במשרד בהתאם לתחום העיסוק של היחידה.

4.10.2.6 להלן מנהלים אשר ישולבו בהיבטי הגנת המידע והסייבר שוטפים:

4.10.2.6.1 מנהל חטיבת טכנולוגיות: ניהול, הטמעה ובקרה אחר כלי, רכיבי ותהליכי הגנת המידע והסייבר במערכות המחשוב של המשרד.

4.10.2.6.2 מנהל משאבי אנוש: דיווח על תנועות עובדים (קליטה, עזיבה ומעבר בין תפקידים) לצורך פתיחת / סגירת הרשאות, טיפול בהיבטי מהימנות עובדים וביצוע מעקב ותיעוד הדרכות.

4.10.2.6.3 היועץ המשפטי: עדכון מנהל תחום הגנת המידע והסייבר ו/או ועדת ההיגוי, אודות שינויים בתקנות ובחוקים הנוגעים להגנת המידע והסייבר וייעוץ בנושאים משפטיים הרלוונטיים להגנת המידע והסייבר במשרד.

**- פנימי -**

מערך סייבר חירום וביטחון I	
פרק:	כללי
מס' פרק:	5
שם הנוהל:	נוהל ניהול משאבי הגנת המידע והסייבר
מס. נוהל:	XXX
ע'י	Page 14 of 14
עודכן ב:	21.09.2014