החלפת מידע

גרסה		שם ומשפחה	תפקיד	חתימה	תאריך
1.0	נכתב על ידי	רונית חייפץ	יועצת אבטחת מידע 2bsecure		31.04.2016
1.0	נבדק על ידי	נחום צור	אבטחת מידע		01.04.2018
1.0	אושר על ידי	מיכאל פרידמן	אחראי מערכות מידע ומיקור חוץ		10.10.2018

<u>מעקב שינויים</u>

מס'	סוג שינוי	מבצע השינוי	תפקיד	תיאור השינוי
	ע	אלון פדרו		עדכון

סוג שינוי: ה – הוספה, מ – מחיקה, ע – עדכון

תוכן עניינים

א. מבוא ..... - 3 -

1. מטרה ..... - 3 -

2. הגדרות ..... - 3 -

3. תחולה ..... - 4 -

4. אחריות ..... - 4 -

ב. שיטה ..... - 5 -

5. הסכמי החלפת מידע ותוכנה ..... - 5 -

6. הסכמי סודיות ..... - 5 -

7. העברת מידע לגורמים חיצוניים ..... - 5 -

8. אבטחת דואר אלקטרוני ..... - 9 -

ג. נספחים ..... - 16 -

9. נספח א' - טופס בקשה להעברת מידע ..... - 16 -

10. נספח ב' - כתב התחייבות מורשה גישה ..... - 20 -

11. נספח ג' – קבלת צרופה באמצעות ממשל זמין ..... - 22 -

12. נספח ד'- סממנים לקיום אפשרי של וירוס או תוכנה מפגעת ..... - 23 -

13. נספח ה' ביטול שימוש בפקודות מאקרו ..... - 25 -

14. נספח ו'- סוגי קבצים האסורים לשימוש ..... - 28 -

א. מבוא

1. מטרה

2.1 הגדרת תהליך הוצאת מידע רגיש אל מחוץ לכותלי רשות מקרקעי ישראל (להלן: "הרשות ו/או "רשות"), תוך מזעור הסיכון לפגיעה בסודיות ושלמות של מידע זה.

2.2 קביעת הנחיות מפורטות לתצורת השימוש בדואר האלקטרוני על ידי בעלי התפקידים ברשות מקרקעי ישראל.

2.3 קביעת עקרונות של אחריות אישית בעת שימוש בדואר האלקטרוני.

3 מסמכים ישימים

3.1 נוהל א8 (א)- ניהול נכסים

3.2 נוהל א8 (ב)- ניהול, הוצאה והשמדת מדיות

3.3 נוהל א9- בקרת גישה

3.4 נוהל א15- אבטחת ספקים

3.5 נוהל א16- ניהול אירועי הגנת סייבר

3.6 מדיניות תעבורת דואר תהיל"ה

3.7 מתודולוגיה לניהול סיכוני הגנת סייבר

3.8 טופס בקשה לקבלת מידע מאת רשות מקרקעי ישראל (גוף ציבורי)

2. הגדרות

5.1 **בעל נכס מידע -** האחראי על המידע, על שינויו ו/או ההשפעה אשר תהיה לאובדנו על הפעילות הארגונית של הרשות.

5.2 **אמצעי זיכרון נתיקים-** אמצעי פיזי המשמש לאחסון (כתיבה וקריאה) של נתונים כדוגמת ה-Disk on Key, External HDD, SD Card, Smart Phone וכיו"ב.

5.3 **מדיה-** מסמכים, מדיה אופטית, מדיה מגנטית וכל אמצעי אחסון אחר.

5.4 **מידע כללי (ניתן לשיתוף ציבורי)-** מידע הפתוח לעיון הציבור. מידע שחשיפתו לציבור לא יגרמו נזק, או מידע אשר יש לפרסמו על-פי דין או שפורסם.

5.5 **מידע פנימי (תפוצה פנימית וגורמי חוץ הקשורים לנושא)-** מידע שחשיפתו לגורמים שאינם מורשים, פגיעה בזמינותו או שיבושו עשויים לגרום נזק לרשות, לגופים ממשלתיים אחרים ו/או לאינטרס הציבורי.

5.6 **מידע חסוי/ חסוי אישי (תפוצה פנימית מוגבלת)-** מידע אשר פגיעה בחסיונו, שלמותו, מהימנותו, זמינותו או שרידותו עלולה לגרום לפגיעה בניהולה התקין של הרשות ו/או משרדי ממשלה אחרים ו/או במדינה או גופים ציבוריים אחרים ו/או לפגוע בפרטיות על פי הגדרת החוק.

5.7 **מידע חסוי ביותר (תפוצה פנימית מצומצמת)-** מידע אשר פגיעה בחסיונו, שלמותו, מהימנותו, זמינותו ושרידותו עלולה לגרום לפגיעה קשה ומתמשכת בניהולה התקין של הרשות ו/או משרדי ממשלה אחרים ו/או במדינה או גופים ציבוריים אחרים.

3. <u>תחולה</u>

3.1. תחולה חלה על כל עובדי רשות מקרקעי ישראל.

4. <u>אחריות</u>

4.1. ממונה הגנת הסייבר

4.2. מנמ"ר

4.3. מנהל הגנת הסייבר

4.4. צוות הגנת הסייבר

4.5. ראש תחום טכנולוגיות

4.6. צוות טכנולוגיות

ב. שיטה

5. הסכמי החלפת מידע ותוכנה

5.1. בכל החלפת תוכנה או מידע עם גורמים צד שלישי יש לכלול בהסכם את הנושאים הבאים:

5.1.1. ציון רמת סיווגו של החומר כפי שנקבע בנוהל ניהול נכסים.

5.1.2. אישור של מנהל הגנת הסייבר להעברה עצמה ולתכולת ההעברה של המידע.

5.1.3. כינון תהליך המבטיח העברה בטוחה של המידע בהתאם לסיווגו.

5.1.4. החלת תהליך ואמצעים המבטיחים את זיהוי השולח, השליח והמקבל.

5.1.5. בקרות מתאימות על תהליך המשלוח (הצפנה, אישור מסירה, תווך מאובטח), בהתאם לרמת החיסיון, אמינות וזמינות המערכת, המידע והגורמים המעורבים בתהליך.

5.1.6. מידע המועבר לגורם צד שלישי יסווג ויישמר לפי נהלי הרשות.

6. הסכמי סודיות

6.1. יש לכלול הסכם סודיות בכל התקשרות של הרשות עם גורם חיצוני שאינו זכאי למידע על פי חוק ובכל מקרה של חלופת מידע בין הרשות לבין גורם אחר.

6.2. על הגורם החיצוני ו/או בעל תפקיד לעמוד בהסכם הסודיות למשך כל תקופת ההתקשרות ו/או הפעילות עם הרשות או מי מטעמה, ללא פגות תוקף.

6.3. התחייבות הגורם החיצוני ו/או העובד לשמירה על מידע רגיש הינה ללא הגבלת זמן.

7. העברת מידע לגורמים חיצוניים

7.1. עקרונות מנחים

7.1.1. הוצאת מידע ממשרדי הרשות עלולה לגרום לשורה של נזקים ולכן בטרם כל בקשה להעברת מידע, על הגורם המבקש למצות את כלל הדרכים לביצוע הפעילות עבורה נדרש המידע, במתחמי הרשות וללא העברת המידע אל מחוץ לרשות.

7.1.2. יחד עם זאת, לעיתים גורמים שונים ברשות פועלים בשיתוף ו/או משתמשים בשירות, המסופק על ידי גופים חיצוניים לביצוע משימות שונות כחלק מהתהליכים העסקיים של הרשות ובמסגרת הגדרת תפקידם. לצורך כך, גורמים מתוך הרשות נדרשים להעביר מידע רלוונטי לגופים אלה (בין השאר, מידע אישי על לקוחות הרשות ועובדיה, מידע על יעדים עסקיים ועוד).

7.1.3. המידע המועבר, מאוחסן ומעובד מחוץ למתחמי הרשות ועלול להיחשף לגורמים בלתי מורשים. אמצעי ההגנה, הבקרה והמעקב המופעלים מחוץ לרשות על ידי הגורמים/ הגופים החיצוניים, עלולים שלא לעמוד ברמה המקובלת והנדרשת ברשות ואינם נמצאים בשליטה ישירה של הרשות.

7.1.4. המשמעויות עיקריות של חשיפת המידע המועבר הן:

7.1.4.1. הפרה אפשרית של החוק הגנת הפרטיות, התשמ"א - 1981 ושל עקרונות שמירת הסודיות.

- חשיפת פריטי מידע אישיים ופיננסיים של לקוחות ועובדים:
  - חוק הגנת הפרטיות, התשמ"א - 1981 אינו משחרר את בעל המאגר ומנהל המאגר מאחריות להגנת הסייבר במקרה שהוא נמצא בידי מורשה הגישה או מחזיק המאגר. מאחריות זו נגזרת חובת פיקוח ואכיפה, כי האחרונים עומדים בחובותיהם בהיבטי אבטחת המידע.

7.1.4.2. חובת הפיקוח הופכת למוגברת ככל שמדובר במידע רגיש יותר או כאשר העברת המידע הינה לפרק זמן ארוך יותר.

7.1.4.3. חשיפת נתונים פיננסיים של הרשות.

7.1.4.4. פרויקטים עתידיים של הרשות, תוך פגיעה בתכנון העסקי של הרשות.

7.1.5. נוהל זה אינו מתייחס למידע על לקוחות בודדים, המועבר על פי נוהלי הרשות לצורך חקירה ע"י גוף חיצוני מוסמך, רשמי או חוקי (כגון: משטרת ישראל, רשויות המס ומי שזכאי לקבלת המידע לפי חוק).

7.2. דרישות סף

7.2.1. בכל מקרה של עבודה עם גורמים חיצוניים וטרם תחילת הפעילות המשותפת עימם, נושא הגנת הסייבר בכלל ושמירת הסודיות בפרט, יוסדר בשלב החוזי, במסגרת הסכם ההתקשרות שנתחם מול גורמים אלו.

7.2.2. במסגרת הסכם ההתקשרות עם גורמים חיצוניים, יש לשמר את הזכות של הרשות לביצוע מעקב ופיקוח באתר הגוף החיצוני, בכל זמן ואופן שימצאו לנכון ע"י נציגי הרשות.

7.2.3. במידה ומועברים לגורם חיצוני פריטי מידע, המהווים חלק ממאגרי המידע של הרשות (מידע אודות לקוחות, עובדים, ספקים ועוד), יש להגדיר בהסכם ההתקשרות את מעמד הגורם החיצוני כמחזיק מאגר מידע ו/או מורשה גישה, עפ"י האמור בחוק הגנת הפרטיות, התשמ"א - 1981 ותקנותיו.

7.2.4. במסגרת הסכם ההתקשרות, יש לחייב את הגורם החיצוני למלא במלואן את כל ההנחיות שתימסרנה מהגורמים המוסמכים ברשות, לאורך כל תקופת ההכנה והביצוע של הפעילות ו/או מתן השירות, במסגרתו יועברו לרשותו נכסי מידע כלשהם, לרבות חתימה על כתב התחייבות בדבר שמירה על סודיות, ביצוע מבדקי מהימנות לעובדים ועוד.

7.2.5. במקרים מסוימים, על פי החלטת מנהל הגנת הסייבר, יוחתמו עובדים ספציפיים כגון עובדי גוף חיצוני, העתידים לספק שירות כלשהו לרשות (ובמסגרת זו, תתאפשר עבורם גישה למאגרי ו/או נכסי המידע של הרשות) על הצהרת שמירת סודיות אישית (ראה נספח ב': "כתב התחייבות בדבר שמירה על סודיות").

7.2.6. במידה ובכוונת הגורם החיצוני לבצע שימוש בשירותי קבלן משנה (צד ג') במסגרת אספקת שירותים לרשות ובמידה ובמסגרת זו נדרשת עבורו גישה למאגרי ו/או נכסי המידע של הרשות, חברת קבלן המשנה תחויב בחתימה על הצהרת שמירת סודיות כתנאי סף להעסקתה בפעילות ולהעברת כל מידע לחזקתה.

7.2.7. אין להעביר מידע תפעולי ו/או עסקי ו/או פרטי לגורם חיצוני לפני חתימה על הסכם עמו, המסדיר את תנאי העברת המידע. בכל מקרה שהמידע נדרש להעברה טרם חתימת ההסכם, יש לקבל אישור חריג והנחיות פרטניות ממנהל הגנת הסייבר ברשות.

7.3. בקשות להעברת מידע

7.3.1. כל העברה חדשה של מידע, המוגדר כבעל רגישות גבוהה, אל מחוץ לכותלי הרשות מחייבת תאום עם מנהל הגנת הסייבר ברשות, קבלת הנחיות רלבנטיות ואישור סופי בכתב (ראה נספח א': "טופס בקשה להעברת מידע").

7.3.2. הבקשה להוצאת מידע בעל רגישות גבוהה תאושר על ידי מנהלו הישיר של מבקש הבקשה, זאת לצרכי הפרדת סמכויות ובקרה.

7.3.3. מנהל הגנת הסייבר ברשות רשאי למנוע הוצאת פריטי מידע, הנחשבים כבעלי רגישות גבוהה, כאשר להערכתו אין הצדקה בהעברתם לגורם מחוץ לרשות. במקרה הצורך, יועלה הנושא לאישור מנהל אגף מערכות מידע ומחשוב ואל הממונה על הגנת הסייבר ברשות.

7.3.4. הנחיות לתצורת העברת המידע בצורה מאובטחת למבקש הבקשה יועברו על ידי מנהל הגנת הסייבר ויונחו על-ידו או מי מטעמו ויפעלו בהתאם לנוהל זה.

7.3.5. כאשר מדובר על בקשה להעברת מידע לגוף ציבורי אחר, על הגוף הציבורי המבקש את המידע למלא טופס בקשה לקבלת מידע מאת רשות מקרקעי ישראל (גוף ציבורי), אשר תיבחן על ידי ועדת ההיגוי להעברת מידע ברמ"י.

7.4. העברת מידע רציפה

7.4.1. עבור מידע, המועבר באופן קבוע ו/או לפרקי זמן ארוכים המוגדרים מראש (כדוגמת מידע המועבר לרכבת ישראל למשך מספר שנים עבור תכנון תוואי רכבת), יש לבצע את תהליכי האישור שלהלן לפני ההתקשרות הראשונה בלבד.

7.5. העברה מידע חד פעמית

7.5.1. העברה חד פעמית של מידע, תתבצע באחת מהדרכים הבאות:

7.5.1.1. העברה ידנית באמצעות מדיה מגנטית/ אופטית/ רכיב זיכרון נתיק ע"י גורם שאושר על ידי רשות מקרקעי ישראל.

7.5.1.2. המידע יועבר באופן מוצפן או מוגן על ידי סיסמא תקנית.

7.5.1.3. העברת המידע עצמו תתבצע ע"י עובדי הרשות/ הגורם החיצוני ובהתאם לנהלי הרשות.

7.5.1.4. כל תהליך העברה אחר יאושר ע"י מנהל הגנת הסייבר.

7.6. הכנת המידע להעברה

7.6.1. לפני העברת המידע לגורם חיצוני, נדרש להקפיד על הנקודות הבאות:

7.6.1.1. יש להיערך להעביר רק את פריטי המידע, שהוגדרו כהכרחיים ונחוצים להשגת מטרת ההעברה ובהיקף המזערי האפשרי ולפרק הזמן הקצר ביותר המתחייב, בהתאם.

7.6.1.2. יש לערבל פריטי מידע מזהים אודות לקוחות או עובדים של הרשות. במידה ולא ניתן לבצע ערבול, יש לקבל אישור בכתב ממנהל הגנת הסייבר לאחר שהנושא נבדק מול המנהל רלוונטי ומנהל מאגר המידע ברשות.

7.6.1.3. יש לבחון בקפדנות את מהימנותו של הספק, ניסיון עבודה קודם הן של רשות מקרקעי ישראל והן של משרדי ממשלה אחרים עמו ואת הסכמיו ו/או התחייבותו לעמוד בכל דרישות החוק.

7.7. אחריות בעל המידע

7.7.1. בעל המידע יישא באחראיות ל:

7.7.1.1. רישום פרטי המידע שהועבר לגורם חיצוני.

7.7.1.2. קבלת אישור מהגורם החיצוני כי המידע התקבל במלואו ובצורה תקינה.

7.7.1.3. ריכוז ושמירה רציפה של התיעוד של העברות המידע המתבצעות ואישורי קבלתו ע"י הגורם החיצוני.

7.7.1.4. בכל מקרה בו חל שינוי בסוג המידע המועבר ו/או באופן העברת ו/או בטכנולוגיה בה משתמש הגורם החיצוני ו/או בשיטת עיבוד המידע ע"י גורם זה, כן שינוי מיקום משרדי הגורם החיצוני ולחילופין, האתר בו מאוחסן המידע בפעול, יש ליידע באופן מידי את מנהל הגנת הסייבר.

7.8. תום תקופת ההתקשרות עם גורם חיצוני

7.8.1. עם סיום ההתקשרות עם הגורם החיצוני יש לבצע את הפעולות הבאות:

7.8.1.1. הודעה לגבי סיום ההתקשרות למנהל הגנת הסייבר.

7.8.1.2. ווידוא כי כלל המידע הוחזר לידי הרשות ולחילופין, הושמד (בהתאם לנוהל א8 (ב)- ניהול, הוצאה והשמדת מדיות) ובכל מקרה, כי בחזקת הגורם החיצוני לא נותר כל פריט מידע ובאתר הגוף החיצוני לא קיימת כל מדיה המכילה חלק או כל מידע של הרשות.

7.9. **ביקורת באתרים חיצוניים**

7.9.1. ביקורות באתרים חיצוניים יבוצעו בהתאם לדרישה של מנהל הגנת הסייבר ברשות.

7.9.2. באחריות מנהל הגנת הסייבר או מי מטעמו לבצע ביקורות תקופתיות באתרים, בהם מוחזק מידע של הרשות ע"י גופים חיצוניים כמפורט בנוהל א15- אבטחת ספקים.

7.9.3. מטרת הביקורת לוודא שהמידע מוחזק בהתאם לדרישות של הרשות וכפי שהוגדר בהסכם ההתקשרות עם הגורם החיצוני.

7.9.4. הביקורות תבוצענה בהתאם לתוכנית העבודה השנתית. חלק מהן תהיינה בידוע הספק מראש וחלקן תיערכנה כביקורות פתע, במקרה הצורך.

8. <u>אבטחת דואר אלקטרוני</u>

8.1. עקרונות שימוש בדואר אלקטרוני

8.1.1. דואר אלקטרוני (דוא"ל) מהווה את התשתית הנפוצה והמהירה ביותר להעברת מידע בין בעלי התפקידים השונים בתוך רשות מקרקעי ישראל וכן, בינם לבין משתמשים מחוץ לרשות כאחד. לאור זאת, מהווה הדואר האלקטרוני כלי עבודה מרכזי בהתנהלות היום-יומית של מרבית בעלי התפקידים ברשות מקרקעי ישראל, דבר המביא עמו תועלות רבות, אך טומן בחובו גם סיכונים לא מבוטלים במספר מישורים, להם נדרש הרשות לתת מענה.

8.1.2. אחד העקרונות המנחים, אשר נועדו למזער את הסיכונים המוזכרים לעיל, הינו כי במהלך השימוש בדואר אלקטרוני תקפים, בנוסף לחוק ולהוראות הדין, כל הנהלים וההוראות הקיימות ברשות בדבר הגנה על זכויות קניין, הזכות לפרטיות, איסור הטרדה מינית, שימוש נאות במשאבי המחשוב של הרשות, הגנת הסייבר ושמירה על סודיות.

8.1.3. שימוש בלתי מורשה/ בלתי חוקי בדואר אלקטרוני, עלול לחשוף את רשות מקרקעי ישראל למצבים שלילים, על כלל ההיבטים הנובעים מכך, לרבות גרימת פגיעה תדמיתית ו/או כלכלית ברשות ואף גרימת עבירה על החוק וחשיפה לקנסות ותביעות משפטיות כפועל היוצא מכך.

8.2. הנחיות כלליות

8.2.1. הדואר האלקטרוני הארגוני מהווה כלי עבודה, הנועד לשמש את בעלי התפקידים השונים ברשות מקרקעי ישראל לביצוע פעילות שוטפת במסגרת תפקידם. אין לעשות בו כל שימוש שלא למטרות עבודה ו/או שימוש העלול לסכן את מערך המחשבים של הרשות.

8.2.2. חל איסור מוחלט למשלוח, קבלה ו/או שמירת כל מידע פרטי בתיבות הדואר של הרשות, אשר אין לו זיקה לעיסוק מקצועי ולהגדרות התפקיד של המשתמש.

8.2.3. כל שימוש בדואר אלקטרוני ייעשה תוך ציות להוראות נוהל זה, שמירה על לשון החוק ולפי הוראות הדין.

8.3. שליחה וקבלה של הודעות דואר אלקטרוני וצרופות

8.3.1. אין לפתוח הודעות דואר אלקטרוני ו/או לאשר קבלת קבצים המצורפים להודעות אלה (הסכמה לקבלת קובץ מצורף – הודעה המתקבלת בצד הנמען מממשל זמין בעת זיהוי צרופה בהודעת דואר אלקטרוני (ראה נספח ג) אשר מקורם בכתובת בלתי מזוהה, לא אמינה ו/או לא מוכרת למשתמש.

8.3.2. עם פתיחת הודעת דואר נכנס, המשתמש יוודא כי לא קיימות התראות אודות איתור וירוס/ פוגען/ קוד זדוני על ידי מערכת האנטי וירוס, המותקנת בתחנת העבודה ו/או בשרתי הדואר הארגוני. יש לשים לב להופעת התראות בחלונות קופצים, הודעות אוטומטיות במייל אודות איתור וירוס והודעות פרטניות מצוות טכנולוגיות בנושא זה.

8.3.3. במידה ודבר דואר המכיל קובץ מצורף, לא התקבל על ידי המשתמש עקב חסימתו במערכות הגנת הסייבר ארגוניות, המשתמש רשאי לפנות לצוות טכנולוגיות/ דלפק סיוע ולבקש לשחרר את דבר הדואר הנחסם. שחרור דבר דואר נחסם יתאפשר לאחר ווידוא כי סוג הקובץ שהתקבל מאושר לשימוש ע"י תחום הגנת הסייבר של הרשות וכן דבר הדואר אינו מכיל פוגען/ וירוס וקוד זדוני. במידה ומדובר בקובץ מסוג שנאסר (ראה נספח ו') לקבלה/שמירה/הפעלה, לא יתאפשר שחרור קובץ זה ותבוצע מחיקתו על ידי צוות טכנולוגיות/ דלפק סיוע.

8.3.3.1. במקרים של קבלת קבצי Microsoft Office באמצעות הדואר האלקטרוני מכתובות דואר חיצוניות לרשות, אין לאפשר הפעלת פקודות מאקרו (ראה נספח ה'), אלא אם כן קיים אישור מפורש ובכתב לכך מצד ראש תחום טכנולוגיות ומנהל הגנת הסייבר.

8.3.4. חל איסור מוחלט על שליחת דואר אלקטרוני, המכיל מידע רגיש בין אם בגוף ההודעה ובין אם בצרופה, לכל גורם בלתי מורשה בתוך או מחוץ לרשות.

8.3.5. חל איסור מוחלט להעביר מידע לגורמים מחוץ לרשות , לרבות גורמים מורשים, המוגדר כרגיש מבחינת הרשות , מבחינת מקבלי השירות ו/או כמוגדר בחוק, באמצעות הדואר האלקטרוני, ללא יישום אמצעי

אבטחה מקובל (כגון הצפנה, חתימה דיגיטאלית, הגנה באמצעות סיסמא ועוד) ומאושר על ידי גורמי אבטחת המידע ברשות מקרקעי ישראל.

8.3.6. אין לשלוח קבצים המכילים תוכנות מפגעות/ וירוסים או כל רכיב אחר, העלול להסב נזק כלשהו למערך המחשוב של הנמען.

8.3.6.1. יש להימנע משימוש בפונקציית 'העברה' (Forward) עבור הודעות דואר אלקטרוני, אשר נתקבלו מגורמים לא מוכרים. בכלל זה מדובר על תכנים פרסומיים המתקבלים ממקור זר, מכתבי שרשרת, הודעות הכוללות קישורים לאתרים חיצוניים ועוד.

8.4. רשימות תפוצה

8.4.1. פרט לרשימות תפוצה, כפי שהוגדרו ברשות מקרקעי ישראל בהתאם למבנה הארגוני, כל משתמש רשאי ליצור רשימת תפוצה פרטית וזאת בתנאי כי:

8.4.1.1. רשימת התפוצה לא תכלול יותר מ-50 כתובות.

8.4.1.2. רשימת התפוצה לא תכלול צבר רשימות תפוצה אחרות, אשר מספר הכתובות הכולל, המרכיב את רשימות תפוצה אלה, עולה על 50 כתובות.

8.4.2. שימוש ברשימות תפוצה ארגוניות יעשה בהגבלות הבאות:

8.4.2.1. שליחת הודעת דואר אלקטרוני בתפוצה כלל ארגונית ("רמי-כל העובדים") תתאפשר לאחר הגשת בקשה סדורה לכך מצד הגורם הרלוונטי ובכפוף לאישור בקשה זו בכתב על ידי מנמ"ר.

8.4.2.2. הבקשה תכלול, לכל הפחות, את הסעיפים הבאים:

- נוסח ההודעה.
- פרטי הגורם המפיץ ולחילופין, הגורם בשמו תופץ ההודעה.
- עילה להפצת ההודעה לכלל הרשות (תקלה רוחבית, ידיעה חשובה ועוד).

8.4.2.3. בעלי תפקידים ברמ"י, אשר משתייכים לקבוצת אבטחה ו/או רשימת תפוצה AllowedToSendALLUsers, מוגדרים כגורמים מורשים לשליחת הודעות דואר אלקטרוני בתפוצה כלל ארגונית. צרוף בעלי תפקידים לקבוצת אבטחה ו/או רשימת תפוצה זו ייעשה

בהתאם להמלצה של מנהל החטיבה/ראש האגף הממונה על בעל התפקיד ובכפוף לאישור המלצה זו בכתב על ידי המנמ"ר.

8.5. גישה לתיבת דואר ארגוניות

8.5.1. רשות מקרקעי ישראל מאפשרת גישת משתמשים לתיבות הדואר הארגוניות במספר תצורות, הנבדלות על פי סוג הגישה (גישה לתיבת הדואר של המשתמש מתוך רשת המחשוב הארגונית ולחילופין, גישה מרשת אינטרנט חיצונית לתיבת הדואר ברשות) והגדרת תפקיד המשתמש ברשות.

8.5.2. גישה מקומית, המתבצעת מתוך רשת המחשוב הארגונית, לתיבת הדואר תתאפשר מתחנת העבודה של המשתמש או תחנת עבודה אחרת, המשויכת לרשות.

8.5.3. גישה מרוחקת לתיבת הדואר, עבור האוכלוסיות המורשות, תתאפשר בתצורות הגישה הבאות:

8.5.3.1. OWA (Outlook Web Access)

8.5.3.2. RDP (Remote Desktop Protocol)

8.5.3.3. AirWatch (עבור טלפונים ניידים)

8.5.3.4. JunosPulse agent

8.5.4. הגישה לתיבת הדואר הארגונית של המשתמש בכל אחת מהתצורות המתוארות מעלה, תותנה בהשלמת תהליך הזדהות חזקה באמצעות כרטיס חכם או סיסמא אישית.

8.6. ניהול ושיתוף תיבות דואר

8.6.1. תיבות הדואר האלקטרוני הארגוני, המוקמות עבור המשתמשים, נועדו לצרכי עבודה בלבד ולא אמורות לשמש כתיבות דואר פרטיות של בעלי התפקידים השונים ברשות מקרקעי ישראל.

8.6.2. אין המשתמשים ברשות רשאים לבצע שימוש בדואר האלקטרוני הארגוני למשלוח וקבלת הודעות וצרופות, המכילות מידע אישי ואין להן כל זיקה לתפקיד המשתמש ברשות.

8.6.3. מתוך כך, הרשות שומרת לעצמה את הזכות לאפשר, על פי הצורך, עיון ו/או שימוש בכל תיבות הדואר הארגוניות (פרטיות, צוותיות, מחלקתיות וכו') לבעלי תפקידים רלוונטיים ברשות מקרקעי ישראל, כפי שיוגדרו על ידי הנהלת הרשות בהתאם לתחום מקצועי, זיקה ארגונית, צורך עסקי ועוד.

8.6.4. לצד האמור לעיל תיבות אלה הינן אישיות, כאשר הרשאות הגישה אליהן כמו גם השימוש בהן, יוגבלו למשתמש המוגדר כבעל התיבה בלבד. בתוך כך, מדובר על מניעת:

8.6.4.1. גישת כל משתמש שאינו מוגדר כבעלים של תיבת בדואר לתוכן התיבה.

8.6.4.2. שליחת הודעות, תוך שימוש בחשבון דואר אלקטרוני אליו משויכת התיבה.

8.6.4.3. העתקה, שינוי ו/או מחיקת דברי דואר אלקטרוני המצויים בתיבה.

8.6.5. מקרים, בהם נדרש לאשר גישת משתמש לתיבת דואר של משתמש אחר, כדוגמת עזיבת עובד, מסירת חומר לצרכי חקירה לידי רשות מוסמכת וכיו"ב יוגדרו כחריגים. במקרים אלה, מתן הרשאות גישה לתיבת הדואר של משתמש עבור צד ג', יותנה ב:

8.6.5.1. אישור מפורש ובכתב מצד המשתמש המוגדר כבעל החשבון, אליו מקושרת תיבת הדואר (קיום סעיף זה מייתר את הצורך במילוי הסעיפים הבאים).

8.6.5.2. חתימת המשתמש, המקבל גישה לתיבת הדואר של משתמש אחר, על הצהרה בדבר אחריות אישית במהלך השימוש בתיבה זו (נדרש בכל מקרה).

8.6.5.3. אישור בקשה למתן גישה לתיבת דואר של משתמש אחר על ידי גורם הנהלה בדרג מנהל מרחב/חטיבה/ראש אגף (בתנאי ולא ניתן לקיים את סעיף 4.6.5.1 לעיל).

8.6.5.4. אישור כתוב מטעם המחלקה המשפטית של הרשות, כי ניתן לאפשר גישה לתיבת הדואר של משתמש למשתמש צד ג'.

8.6.6. הקמת תיבת דואר משותפת (כגון: תיבת דואר מחלקתית) תיעשה בהתאם לבקשה סדורה לכך מצד הגורם הרלוונטי ובכפוף לאישור בקשה זו בכתב על ידי ראש תחום טכנולוגיות או גורם מטעמו. בקשה זו תכלול, לכל הפחות את הפרטים הבאים:

8.6.6.1. מטרת הקמת התיבה המשותפת.

8.6.6.2. פרטי המשתמשים, עבורם נדרש לתת הרשאות גישה לתיבה זו.

8.7. ניהול ושיתוף יומנים

8.7.1. מלבד תיבת הדואר האישית, לכל עובד בעל חשבון דואר אלקטרוני מוגדר יומן אישי, המהווה כלי לניהול לוחות הזמנים והפעילות של המשתמש במסגרת תפקידו ברשות.

8.7.2. כל משתמש רשאי לשתף את יומנו האישי עם משתמשים נוספים ובתנאי בעלי תפקידים אלה נמנים עם משתמשי הרשות בלבד.

8.7.3. משתמש, המשתף את יומנו האישי עם משתמשים אחרים ברשות בכל תצורה (הרשאות עיון או ניהול), נוטל על עצמו את האחריות והסיכון שבחשיפת מידע בעל רגישות אישית או ארגונית כגון: נושאי פגישה רגישים, בעלי תפקידים המשתתפים בפגישה וכיו"ב, העלול להיחשף למשתמשים אחרים בעלי הרשאות ביומנו.

8.8. אירועים חריגים

8.8.1.1. עם קבלה ו/או פתיחה של הודעת דואר אלקטרוני וצרופתה, על המשתמשים להיות ערים להודעות וההתרעות המופקות ממערכות אבטחת המידע (כגון: Fire Wall,Anti-Virus ועוד) אודות איתור או המצאות תוכנות מפגעות בתחנת העבודה ואף למצבים, בהם ישנו חשד בלבד לקיום תוכנה מסוג זה.

8.8.2. במקרה של חשד לקיום וירוס/ קוד זדוני/ פוגען מסוג כלשהו בתחנת העבודה של המשתמש ו/או ברשת המחשבים של הרשות, כתוצאה מאיתור התנהגות/ תופעות לא שגרתיות (ראה נספח ד') המתרחשות במהלך/ כתוצאה משימוש בדואר האלקטרוני, לרבות פתיחת הודעה ו/או קובץ מצורף, המשתמש יבצע את הפעולות הבאות:

8.8.2.1. דיווח באופן מיידי לדלפק סיוע/ צוות הפעלה במרחב אשר יפתח קריאה במערכת Sysaid וישייך אותה לצוות הגנת הסייבר, המספק תמיכה טכנית תפעולית בעת התרחשות אירועים חריגים, העלולים לסכן את המערכות ו/או את רשת המחשבים של הרשות. דלפק סיוע/ צוות הפעלה יבצע הערכת מצב ראשונית ובמידה ויוחלט כי מדובר באירוע אבטחתי, המשך הטיפול ייעשה מול צוות טכנולוגיות על פי נוהל א16- ניהול אירועי הגנת סייבר.

8.8.2.2. ניתוק המחשב ה"נגוע" מהרשת הארגונית ומרשת האינטרנט (במידת האפשר) על ידי ניתוק פיזי של כבל הרשת מנקודת התקשורת.

8.8.2.3. יש להימנע מהעברת מידע למחשבים אחרים ברשת המחשוב הארגונית ומחשבי Stand Alone, עד להשלמת הערכת מצב ראשונית על ידי הצוותים הטכניים וקבלת אישור מפורש לכך.

8.8.3. חל איסור מוחלט להמשיך ולעבוד במחשב ה"נגוע" טרם השלמת תהליכי תחקור טכני (Forensics) והשלמת הטיפול לכדי הגדרתו כמחשב "נקי" בהובלת תחום טכנולוגיות ותחום הגנת הסייבר.

8.9. מקורות מידע נוספים

8.9.1. בהיות הרשות משרד ממשלתי, שירותי שליחה/ קבלה של הודעות דואר אלקטרוני אל/מאת גורמים חיצוניים, בהתאמה, מבוססים בחלקם על תשתית המתוחזקת והמנוהלת על ידי ממשל זמין. הנחיות רלוונטיות נוספות, הנוגעות לדואר אלקטרוני, ניתן למצוא במסמך "מדיניות תעבורת דואר תהיל"ה", כפי שפורסם בתאריך 13.08.2012.

8.10. אחריות אישית וייצוגית

8.10.1. למען הסר ספק, בעת שימוש בדואר אלקטרוני, נחשב כל משתמש ברשות כגורם מייצג של הרשות כלפי כל גוף החיצוני.

8.10.2. בהיבט האחריות האישית ו/או ייצוג הרשות כלפי כל גוף חיצוני, אין העברת מידע בדואר אלקטרוני שונה בכל צורה שהיא מהעברת המידע במסמכים קשיחים.

ג. נספחים

9. נספח א' - טופס בקשה להעברת מידע

תאריך הוצאת הבקשה: _____

פרטי המבקש

שם משפחה: _____

שם פרטי: _____

תפקיד: _____

המטרה לשמה מבוצעת הוצאת המידע

_____

_____

_____

היעד אליו מוצא המידע

שם חברה/ארגון: _____

שם איש קשר: _____

טלפון: _____

יעד ביצוע העברה

תאריך: _____/_____/_____

סווג המידע

שם המערכת ממנה נגזר/יוצא המידע: _____

האם המידע מכיל פרטים אישיים של לקוחות ☐ כן ☐ לא

האם המידע מכיל נתונים רפואיים ☐ כן ☐ לא

האם המידע מכיל נתונים פיננסיים ☐ כן ☐ לא

האם המידע מכיל נתוני זיהוי חד ערכיים (שם משתמש ו/או סיסמא) ☐ כן ☐ לא

במקרה אחר נא פרט:

_____

_____

נפח המידע (גודל פיזי ב-GB/MB): _____

<u>תדירות העברת המידע</u>

☐ חד פעמית

☐ רציפה

<u>טופס בקשה להעברת מידע חד פעמית:</u>

<u>מהות הדרישה</u>

☐ תחזוקה/תיקון ☐ עסקית ☐ משפטית ☐ אחר_____

<u>אמצעי ההעברה</u>

☐ מדיה מגנטית ☐ מדיה אופטית ☐ רכיב זיכרון ☐ עותק כשיח (מסמך)

☐ אחר: _____

<u>העברה בגין</u>

☐ בקשת לקוח ☐ בקשת רשות ממשלתית ☐ בקשת גוף עסקי/פרטי

☐ אחר: _____

<u>במקרה של הוצאה לתחזוקה/תיקון</u>

פירוט נסיבות לאי ביצוע הפעילות באתר הרשות

_____

_____

_____

_____

האם בוצע ערבול נתוני הזדהות ופרטים אישיים של לקוחות?

☐ כן ☐ לא ניתן לבצע. הסבר: _____

האם בוצע שינוי ערכים מזהים לפני הוצאתם?

☐ כן ☐ לא ניתן לבצע. הסבר: _____

האם בוצעה "גזירת" כמות המידע בצורה המינימלית?

☐ כן ☐ לא ניתן לבצע. הסבר: _____

<u>טופס בקשה להעברת מידע רציפה</u>

האם קיים תהליך מיכון אוטומטי עבור העברת המידע?

☐ **קיים תהליך מיכון אוטומטי**

פרטי איש קשר בחברה

שם ומשפחה: _____

תפקיד: _____

טלפון: _____

* יש לצרף אפיון התהליך לבקשה, כך שיכלול עמידה בדרישות הגנת הסייבר כגון: הצפנה, כספת וירטואלית או כל אמצעי מקובל אחר.

☐ **לא קיים תהליך מיכון אוטומטי**

פרט_____

_____

<u>אמצעי ההעברה</u>

☐ מדיה מגנטית ☐ מדיה אופטית ☐ רכיב זיכרון ☐ עותק כשיח (מסמך)

☐ אחר: _____

<u>העברה בגין</u>

☐ בקשת לקוח ☐ בקשת רשות ממשלתית ☐ בקשת גוף עסקי/פרטי

☐ אחר: _____

<u>פרטי מבצע ההעברה בפועל</u>

שם ומשפחה: _____

טלפון: _____

<u>אישורים</u>

_____	_____
חתימת המבקש	תאריך
_____	_____
חתימת גורם הגנת הסייבר	תאריך
_____	_____
חתימת מנהל אגף מערכות מידע ומחשוב	תאריך

10. נספח ב' - כתב התחייבות מורשה גישה

לכבוד: רשות מקרקעי ישראל תאריך: _____

א.נ.,

הנדון: **כתב התחייבות בדבר שמירה על סודיות**

הואיל: ואני עובד של _____ (להלן: "**החברה**"), אשר עתידה לספק לרשות מקרקעי ישראל (להלן: "**הרשות**") שירותים שונים, לרבות שרותי מחשוב.

והואיל: וידוע לי כי לצורך ביצוע תפקידי, החברה נדרשת לה גישה למידע המצוי במערכת המחשב של הרשות, בין היתר מידע שחלה עליכם לגביו חובת סודיות בין עפ"י דין ובין עפ"י הסכם (להלן: "**המידע**").

והואיל: והחברה מבקשת להשתמש בשירותי לצורך ביצוע חלק מהמטלות אשר מצריכות גישה ישירה למידע.

והואיל: וידוע לי כי הסכמתם לאפשר לחברה גישה למידע גם על סמך הצהרותיי והתחייבויותיי שלהלן.

לפיכך אנו מצהירים ומתחייבים בזה כלפיכם כדלקמן:

1. המבוא לכתב זה מהווה חלק בלתי נפרד ממנו.
2. הנני מצהיר כי הגישה למידע בכל צורה שהיא תינתן לי אך ורק לצורך מילוי תפקידי וכי אסור לי לעשות שימוש כלשהו במידע שיגיע לרשותי בכל דרך וצורה שהיא.
3. הנני מתחייב לשמור בסוד כל מידע שיגיע אלי במסגרת ביצוע תפקידי ובמהלכו בין אם הגיע אלי במכוון ובין אם התגלה באקראי, ולא אמסור ו/או אגלה לצדדים שלישיים כלשהם שום מידע (בין בעל פה, בין בכתב, ובין בכל אופן אחר) שנתקבל כאמור.
4. הנני מתחייב להימנע מלשמור ברשותי כל מידע שיגיע אלי, אלא במידה שהדבר נחוץ לצורך ביצוע עבודת החברה עבורכם ואך ורק למשך התקופה שהדבר דרוש לביצועה וכן לנקוט בכל האמצעים שהחברה תעמיד למניעת חשיפתו, כולו או חלקו, בפני כל אדם שלא קיבל הרשאה לשימוש בגישה ישירה לאחר שחתם על התחייבות לשמירה על סודיות בנוסח שיאושר על ידכם בכתב (להלן: "**מורשה גישה**").

5. הנני מתחייב להשיב לחברה או לכם מיד עפ"י דרישתכם הראשונה בכתב ו/או מיד עם סיום ביצוע עבודת החברה עבורכם או עם ביטול הרשאתנו לגישה לפי המוקדם מביניהם, כל מידע שיהא מצוי אצלי שנתקבל מכם בין במסמך בין במדיה מגנטית ובין אחרת.
6. אני מתחייב שלא להעתיק או להעביר כל חומר מגנטי או מודפס ממערכות המחשב שלכם אל מחשב חברה אחרת כלשהי.
7. ידוע לי שהפרת התחייבותי על פי כתב זה או כל חלק מהן עלולה להיחשב כעבירה פלילית ו/או כעוולה אזרחית על פי הוראות הדין, לרבות חוק הגנת הפרטיות, התשמ"א - 1981, וכי כל הפרה כזו תיחשב גם כהפרה יסודית של ההסכמים שביניכם לבין החברה.

ולראיה באתי על החתום היום _____

חתימת העובד

פרטי העובד

שם _____

ת.ז _____

תפקיד_____

אני הח"מ _____ מאשר כי מסמך זה נחתם בפני היום לאחר שזיהיתי את החותם, אימתי את פרטיו והסברתי לו את מהות ההצהרות וההתחייבויות הכלולות במסמך זה.

_____ _____ _____

תאריך שם ומשפחה חתימה וחותמת

11. נספח ג' – קבלת צרופה באמצעות ממשל זמין

פרויקט תהילה - מערכת דואר אלקטרוני מאובטחת

לקוח/ה יקר/ה!
במערכת הדואר של תהילה התקבלה הודעת דואר עם צרופה חשודה
Dear customer!
A message with a suspicious attachment has been received in tehila mail system

שדות לזיהוי השולח ופרטי הצרופה →

המקור השולח: anyone@anything.co.il
שכותרתו היא: 31.3.2014 file name
ועם הקבצים המצורפים הבאים: ; zip.31.3.2014-file name

אם הינך מזהה את השולח, ומצפה להודעה זו, באפשרותך לקבל את ההודעה ע"י הקשה על הקישור

הסכמה לקליטת הצרופה → מסכים

אם אינך מצפה להודעה זו ואינך מעוניין לקבלה, בבקשה אל תעשה דבר.

קבלת הודעות עם צרופות לא מזוהות, מסכנת את הרשת המשרדית. אנא פעל בזהירות!

Mail sender:
Subject: file name 31.3.2014
And with the following attached files: ; file name 31.3.2014-.zip

If you recognize the sender, and you are expecting this email, you can accept the message by clicking on agree

If you are not expecting this email and you are not interested to get it, please do nothing.

Receiving messages with unrecognized attached files could be dangerous for the local net. Please act safe.

לידיעתך, הודעת הדואר תשמר בשרת למשך 7 ימים ולאחר מכן תמחק אוטומטית.
Please note, the message will be on the server for 7 days and then automatically removed.

צוות תהיל"ה לשרותך. טלפון: 6664646 - 02 , דוא"ל: noc@tehila.gov.il

12. נספח ד'- סממנים לקיום אפשרי של וירוס או תוכנה מפגעת

סממנים לקיום אפשרי של וירוס או תוכנה מפגעת

לצד מגוון מערכות אבטחת המידע, המוטמעות והמופעלות ברשות להגנה על משאבי המחשוב של רשות מקרקעי ישראל מפני האיומים השונים, אין מערכות אלה מספקות הגנה הרמטית מפני כלל האיומים הקיימים ומוסיפים להתפתח מדי יום בקצב הולך וגובר.

אי לכך, לא כל וירוס, 'רוגלה', תוכנה מפגעת או כל איום אבטחתי אחר, מאותר ונחסם על ידי מערכות אבטחה אלה ובמקרים מסוימים, איתור המצאות פוגען ואף הצבעה על חשד לפגיעה במערך המחשוב הארגוני נתון בידי המשתמשים.

בכדי לסייע למשתמש באיתור מקרים אלה, להלן מספר סממנים, העשויים לאפיין תחנת עבודה/רשת מחשבים "נגועה" כתוצאה מחדירת וירוס או כל פוגען אחר:

1. **הודעות קופצות (Pop Up)**

הופעת הודעות בעלות תכנים פרסומיים ו/או אופי התראתי על מסך המחשב. הופעת הודעות אלה מאופיינת בפרסום תכנים למבוגרים, אתרים אינטרנטיים (לרבות אתרים שהמשתמש לא ניגש אליהם בעבר), הצעות להורדת והתקנת תוכנות אבטחה (AntiVirus, AntiSpam, Performance Enhancer) המשמשות בפועל כ'רוגלות', תוך הצגת התראה כוזבת על קיום וירוס בתחנת העבודה.

2. **ביצועי מחשב איטיים מהרגיל**

תוכנות פוגעניות נוטות להריץ פקודות ולהפעיל שירותים שונים בתחנת העבודה ה"נגועה", כאשר הם מתרחשים ברקע וללא ידיעת המשתמש. פעולות אלה לרוב נדרשות למשאבי עיבוד (Processing Resources) נרחבים של תחנת העבודה, דבר הגורר איטיות קיצונית בביצוע פעולות שגרתיות על ידי המשתמש בתחנת העבודה.

3. **"קיפאון", קריסה ואתחול יישומים ותחנות עבודה**

בתהליך התפשטות התוכנה המפגעת בתחנת העבודה ו/או ברשת המחשבים הארגונית, ככלל מבצע הפוגען גישה ואף שינוי של קבצי מערכת ההפעלה ו/או קבצים חשובים ביישומים השונים המותקנים בתחנת העבודה. שינויים אלה עלולים לשבש את פעילותו התקינה של היישום ה"נגוע" וכן, של תחנת העבודה בכללותה. שיבושים אלה מאופיינים לרוב בגרימת קריסות חוזרות ונשנות ו/או ביצוע פעולות אתחול בלתי נשלטות ולעיתים רצופות (loop) של היישום/תחנת העבודה ולחילופין, 'תקיעה' כתוצאה מהפעלת היישום, ביצוע פעולה כלשהי ביישום, פתיחת קובץ מסויים וביצוע פעולות שגרתיות נוספות.

4. **שינוי הגדרות אבטחת מידע**

מאפיין נוסף של קיום תוכנה מפגעת בתחנת העבודה הינו שינוי הגדרות אבטחה שהמשתמש לא יזם בעצמו. במסגרת זו נכלל נטרול תוכנת ה-Anti Virus המותקנת בתחנה, שינוי הגדרות ה-FW המקומי לתצורה מתירנית ועד כדי ביטולו, שינוי הרשאות גישה לכוננים/תיקיות/קבצים מוגנים ופעולות נוספות כגון אלה.

5. הודעות שגיאה

שינויים, המבוצעים על ידי התוכנות המפגעות בהרשאות הגישה, בקבצי המערכת ו/או בקבצי הנתונים בתחנות העבודה ו/או הרשת הארגונית, מובילים לעיתים קרובות למצב, בו היישום לא מסוגל לגשת כהלכה לקובץ היעד ו/או לתוכנו ומציג בעקבות כך הודעת שגיאה. הודעות אלה מצביעות ככלל על השחתת מידע (Data corruption), מניעת הרשאה לניהול יישומים (Task Manager disabled), מניעת הרשאה להרצת פקודות (regedit command is disabled ו-msconfig command is disabled), מניעת גישה לכוננים/תיקיות/קבצים (Access Restriction) ועוד.

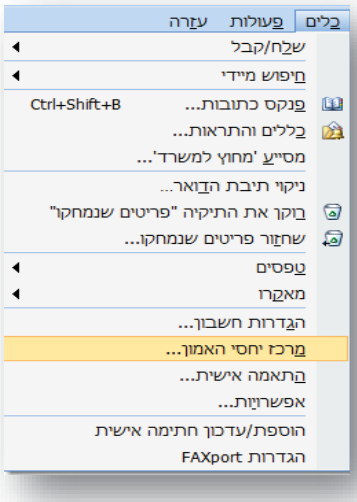
6. שינוי נתונים

סממן נוסף לקיום תוכנה מפגעת בתחנת העבודה ו/או ברשת המחשוב הארגונית הינו הופעת/העלמות של קבצים/תיקיות, אשר לא נוצרו/נמחקו על ידי המשתמש או גורם מורשה אחר (כגון: צוות תמיכה טכנית), שינוי בנפח הקבצים או בתאריך יצירתם, שינוי מיקום שמירתם ברשת וכו'.

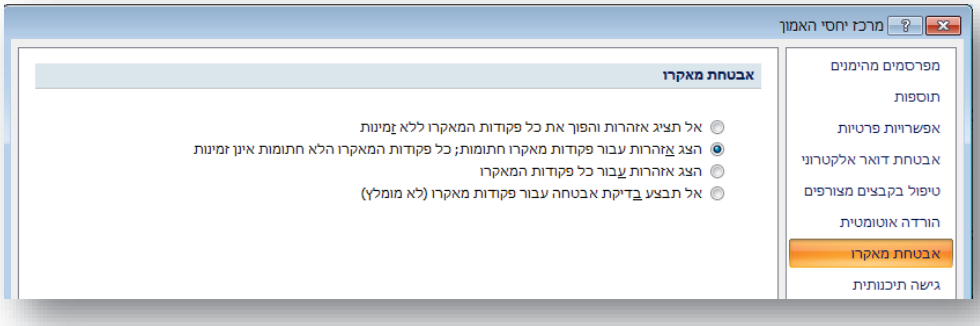
13. נספח ה' ביטול שימוש בפקודות מאקרו

ביטול שימוש בפקודות מאקרו

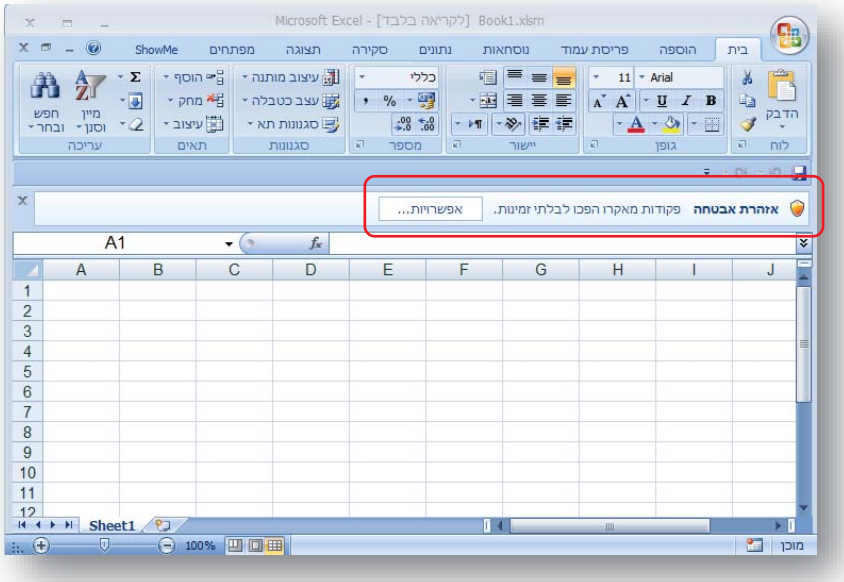
1. כל קובץ, הנשלח לכתובת הדואר האלקטרוני של משתמש והמכיל פקודות מאקרו, עלול לטמון בחובו קוד זדוני ולהוות חשיפה אבטחתית בעלת פוטנציאל נזק רב לרשות.
2. זאת, היות ובאפשרותו של הגורם הזדוני לנצל את היכולת הניתנת על ידי שימוש בשפת תכנות VBA (Visual Basic for Applications) לכתיבת קוד/רצף פקודות, אשר יופעלו בעת פתיחת הקובץ בו הן מוטמעות, על ידי היישום הרלוונטי (ככלל יישומי Microsoft Office). בעזרת פקודות אלה, ניתן לגשת למגוון משאבים (לרבות: מערכת ההפעלה וקבצים מאוחסנים) וכן לבצע מגוון רחב של פעולות בתחנת העבודה של המשתמש ואף ברשת הארגונית (לרבות: העתקה, מחיקה ושינוי קבצים, הוצאת מידע החוצה ללא ידיעת המשתמש, הורדת והתקנת תוכנות מפגעות ללא ידיעת משתמש ועוד).
3. על מנת למנוע את אפשרות קבלת/הרצת פקודות מאקרו באופן אוטומטי, יש לבצע את השלבים הבאים:
   א. ביישום ה-Outlook יש לגשת לסימניית "כלים" שבסרגל הכלים ולבחור ב"מרכז יחסי האמון":



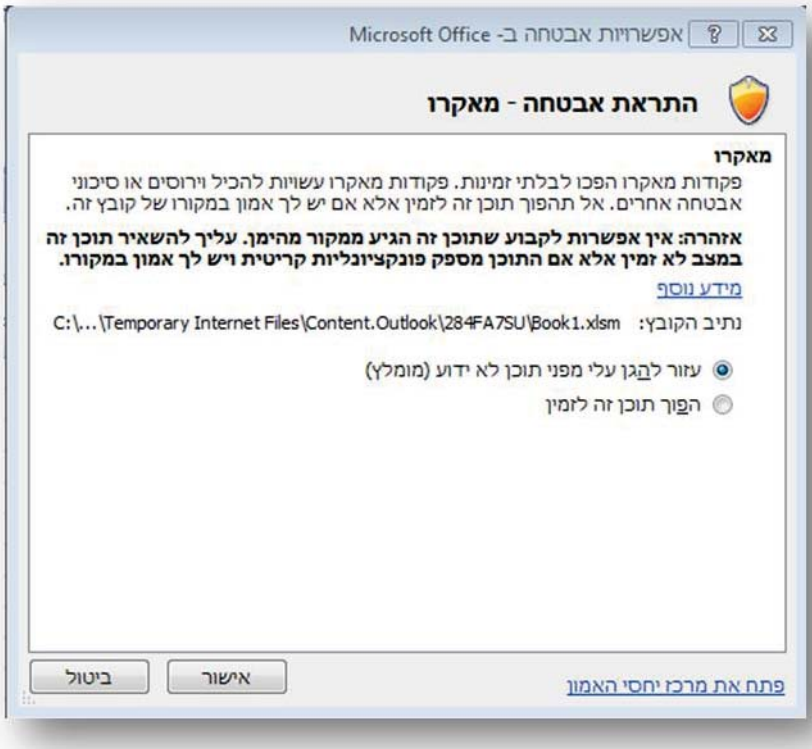
לאחר מכן, יש לבחור בתפריט "אבטחת מאקרו" ולסמן את האפשרות השנייה "הצג הזהרה עבור פקודות מאקרו...":



ב. ביישומי Microsoft Office יש לבצע תהליך דומה, בעת קבלת קובץ עם סיומת (Extension), המצביעה על קיום פקודות מאקרו (כגון : xlsm). עם פתיחת הקובץ, תופיע הודעה "**אזהרת אבטחה** פקודות מאקרו הפכו לבלתי זמינות".



מצב זה הינו תקין, אך מומלץ לבחור ב"אפשרויות..." ולבחור באפשרות הראשונה "עזור להגן עלי מפני תוכן לא ידוע" :



4. כברירת מחדל, בצד המשתמשים של רשות מקרקעי ישראל, הפעלת פקודות מאקרו תהיה חסומה ב-Outlook ובייישומי Microsoft Office.
5. אישור להפעלת פקודות מאקרו יינתן באופן פרטני ובכתב על ידי ראש תחום טכנולוגיות וגורם אבטחת מידע בכפוף להגשת בקשה סדורה מצד המשתמש.

14. נספח ו'- סוגי קבצים האסורים לשימוש

סוגי קבצים האסורים לשימוש

להלן רשימת סוגי סיומות (extension) של קבצים, הנפוצים כתשתית להפצת וירוסים/קודים זדוניים ותוכנות פוגעניות:

*.ADE	*.ISP	*.REG
*.ADP	*.JS	*.SCF
*.APP	*.JSE	*.SCR
*.ASP	*.JSP	*.SCT
*.ASX	*.KSH	*.SHB
*.BAS	*.LNK	*.SHD
*.BAT	*.MDA	*.SHE
*.CAB	*.MDB	*.SHN
*.CHM	*.MDE	*.SHS
*.CMD	*.MDT	*.URL
*.COM	*.MDW	*.VB
*.CPL	*.MDZ	*.VBE
*.CRT	*.MSC	*.VBS
*.CSH	*.MSI	*.VSS
*.EXE	*.MSP	*.VST
*.FXP	*.MST	*.VSW
*.HLP	*.OPS	*.WSC
*.HTA	*.PCD	*.WSF
*.INF	*.PIF	*.WSH
*.INS	*.PRF	