כללי הגנת הסייבר לבעל תפקיד ברשות מקרקעי ישראל

גרסה		שם ומשפחה	תפקיד	חתימ	תאריך
1.0	נכתב על ידי	סיסי הכהן	יועצת אבטחת מידע 2bsecure		10.10.2016
1.0	נבדק על ידי	נחום צור	צוות אבטחת מידע		01.04.2018
	אושר על ידי				

<u>מעקב שינויים</u>

מס'	סוג שינוי	מבצע השינוי	תפקיד	תיאור השינוי
1	ע	סיסי הכהן	יועצת אבטחת מידע 2bsecure	עדכון והתאמה לתקן ISO 27001

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

תוכן עניינים

א. מבוא ..... - 3 -

1. מטרה ..... - 3 -

2. הגדרות ..... - 3 -

ב. כללי ..... - 4 -

4. הגדרות ..... - 4 -

5. תחולה ..... - 6 -

6. אחריות ..... - 6 -

ב. שיטה ..... - 7 -

7. עקרונות ..... - 7 -

8. ניהול טלפונים חכמים ..... - 7 -

9. מחיקת נתונים מרחוק ..... - 9 -

10. תפעול מערכת MDM ..... - 10 -

11. פרטיות משתמשים ..... - 11 -

ג. נספחים ..... - 14 -

13.1. נספח א- טופס אחריות אישית- שימוש במכשירי טלפון חכמים ומחשבים ניידים המתחברים לרשת רשות מקרקעי ישראל. ..... - 14 -

13.2. נספח ב'- בדיקת תאימות טלפון חכם ..... - 17 -

13.3. נספח ג- קבוצות AW ..... - 19 -

א. מבוא

1. <u>מטרה</u>

1.1. מסמך זה מפרט את מדיניות רשות מקרקעי ישראל (להלן: "הרשות") בנוגע לשמירה והגנה על המידע העסקי המסווג של רשות מקרקעי ישראל ולקוחותיה.

1.2. עובדי רשות מקרקעי ישראל עושים שימוש יום יומי במערכות ותשתיות הארגון. כתוצאה מעבודה לא נכונה על מערכות המידע והמחשוב עלולות להיווצר פרצות בהיבטי הגנת הסייבר אשר יבואו לידי ביטוי בפגיעה בהגנה על הסודיות וכן בשלמות וזמינות המידע ברשות. בנוהל זה מפורטות מדיניות והנחיות ייעודיות לעובדים ברשות מקרקעי ישראל ולעובדי חוץ בעלי גישה למערכות של רשות מקרקעי ישראל, כיצד להתנהל נכון בהיבטים אלה, כמו גם בהיבטי שימוש מאובטח במשאבי הארגון.

2. <u>הגדרות</u>

2.1. **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.

2.2. **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.

2.3. **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.

2.4. **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.

2.5. **עקרון "הצורך לדעת"-** עקרון מנחה באבטחת מידע לפיו יש לאפשר לכל משתמש לגשת רק למידע אליו הוא זקוק, לצורך מילוי תפקידו.

2.6. **רכיבי מחשוב ניידים-** מכשירי מחשוב ניידים כגון: מחשב נייד (לפטופ), טלפון חכם (סמארטפון), מחשבי לוח (טאבלט) וכד'.

ב. כללי הגנת סייבר לעובד רשות מקרקעי ישראל

3. <u>שמירה על סודיות המידע</u>

3.1. מערכות המידע והמחשוב של הארגון מאחסנות נתונים רבים הקשורים לקרקעות ולבעליהן. זכרו! חל איסור מוחלט למסור כל מידע הקשור לצנעת הפרט ממאגרי המידע של הארגון לגורמים לא מורשים.

3.2. עם כניסתך לתפקיד, הנך נדרש לחתום על הסכם סודיות, במסגרת תהליך הקליטה ברשות.

3.3. חל איסור על גילוי מידע ו/ או שימוש עסקי מסווג שהגיע אליך במסגרת עבודתך ברשות, אלא לצורך ביצוע עבודתך ובהתאם לכללים אלה.

4. <u>העברת מידע</u>

4.1. הוצאת מידע ממשרדי רשות מקרקעי ישראל עלולה לגרום לשורה של נזקים ולכן, יש למצות את כלל הדרכים לביצוע העבודה, עבורה נדרש המידע, במתחמי הרשות וללא העברת המידע אל מחוץ לארגון, בטרם כל בקשה להעברת מידע.

4.2. כל העברת מידע, המסווג כמידע פנימי/ חסוי/ חסוי אישי / חסוי ביותר, אל מחוץ לכותלי הרשות מחייבת לקבל אישור ממנהלך הישיר. הוצאת המידע תתאפשר רק לאחר קבלת הנחיות רלוונטיות ואישור סופי בכתב (ראה נספח א': "טופס בקשה להעברת מידע").

4.3. העברת מידע חד פעמית המחייבת מסירת נתוני מקור/ אמת, תתבצע באחת מהדרכים הבאות:

4.3.1. במידת האפשר, המידע יועבר באופן מוצפן או מוגן על ידי סיסמא תקנית.

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

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

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

4.4. במקרה של ספק, במקרים חריגים או במקרה בו לא ידועה לך רמת סיווג המידע, יש לפנות למנהל הגנת הסייבר.

4.5. לפני העברת המידע לגורם חיצוני, עליך להקפיד על הנקודות הבאות:

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

4.5.2. יש לבחון בקפדנות את מהימנותו של הגורם החיצוני המבקש לקבל את המידע, ניסיון עבודה קודם הן של רשות מקרקעי ישראל והן של משרדי ממשלה אחרים עמו ואת הסכמיו ו/או התחייבותו לעמוד בכל דרישות החוק.

5. כניסת עובדים, מבקרים ונותני שירות למתחמי רשות מקרקעי ישראל

5.1.1. באחריותך לאשר את כניסתם של המבקרים/ נותני השירות אותם אתה מקבל, וכן לוודא כי הינם מלווים מרגע כניסתם ועד ליציאתם ממתחמי הרשות.

5.1.2. בהמשך יחויב כל מבקר / אורח לנוע במרחבי מתחמי הרשות עם תג / שרוך המציין כי הינם מבקרים. האחריות לוודא כי הנחיה זו מקוימת הינה על מזמין השירות / המבקרים.

5.1.3. בעת שהותך במתחמי העבודה של הרשות עליך לשאת תג עובד.

5.1.4. תג העובד הנו אישי ואין להעבירו לאף אדם אחר.

5.1.5. במקרה של אובדן / גניבת תג העובד עליך לדווח לדלפק סיוע ו/או לקב"ט.

5.1.6. עליך להיות ערני ולשים לב שגורמים שאינם מורשים לא נכנסים למתחמי הרשות. במידה ונתקלת בגורם שאינו מורשה יש לדווח מידית לקב"ט.

6. מדיניות שולחן נקי

6.1. אל תשאיר מסמכים ומידע בסביבת העבודה ללא השגחה. בעת היעדרות ממושכת ובתום יום העבודה עליך לאחסן מסמכים באופן מסודר במגירתך האישית ו/ או בארון נעול או לנעול את החדר.

6.2. עליך לגרוס מסמכים שאין בהם צורך באמצעות המגרסות המיועדות לכך, אין לצבור מסמכים שלא לצורך במתחם העבודה.

6.3. אל תשאיר את המפתחות למגירה/ ארון בתוך חור המנעול שלהם או במקום גלוי בסביבת העבודה.

6.4. אל תשאיר הדפסות, העתקי פקסים, מסמכים מצולמים באזור ההדפסה הציבורי.

6.5. אין לשמור סיסמאות בסמיכות לשולחן העבודה או עמדת המחשב.

6.6. במידה ויש אפשרות יש לנעול את החדר בעת עזיבתו.

7. <u>גישה וסיסמאות למערכות המידע של רשות מקרקעי ישראל</u>

7.1. הרשאות השימוש במערכות המידע והרשת של רשות מקרקעי ישראל מוגדרות בהתאם לתפקיד ועל פי עקרון "הצורך לדעת".

7.2. הנך אחראי על כל פעולה המתבצעת תחת שם המשמש שלך.

7.3. כל גישה למערכות המידע ברשות מקרקעי ישראל מותנית בהזנת שם משתמש אישי וסיסמא אישית, לשם אימות זהותך. כאשר במערכות רגישות נדרש בנוסף לכך גם אמצעי זיהוי חכם.

7.4. הסיסמא למחשבי הרשות הינה אישית ואין להעבירה לאף גורם אחר - יש לשמור אותה בסודיות. בכל מקרה אין לשמור את הסיסמא בקרבת המחשב.

7.5. אין להיכנס למחשבי הרשות באמצעות שם משתמש וסיסמא של עובד אחר, פעולה זו הינה בגדר התחזות.

7.6. על הסיסמא להיות שונה משם המשתמש (Username), שם פרטי או שם משפחה.

7.7. אין לבחור סיסמאות טריוויאליות (כגון: שמו של בן/בת זוג ו/או ילדיו וכו').

7.8. אין לבחור סיסמא המורכבת מרצף מקשים שעל המקלדת, בעברית או באנגלית (כגון: שדגכ, qwerty וכו').

7.9. אין לעשות שימוש במילים מוכרות (כגון: "סיסמא" וכו').

7.10. חוזק הסיסמה נקבע על פי אורכה. לכן, ככל שהסיסמה תהיה ארוכה יותר (גם ללא מספרים או סימנים מיוחדים) היא תהיה חזקה יותר. בכל מקרה, אורך הסיסמא יהיה מורכב לפחות מ-8 תווים.

7.11. במידה והסיסמה היא 8 תווים, נדרש לחזק אותה ע"י שילוב של <u>3 פרמטרים</u> לפחות מתוך הרשימה הבאה:

7.11.1. אות גדולה אחת לפחות

7.11.2. אות קטנה אחת לפחות

7.11.3. תו מיוחד אחד לפחות (&, * ? וכו')

7.11.4. ספרה אחת לפחות

7.12. יש להחליף סיסמה כל 180 יום (מערכות המידע והמחשוב של הרשות יתריעו טרם תום התקופה, לא תתאפשר המשך עבודה לאחר 180 יום מבלי החלפת הסיסמא).

7.13. אם נודע לך שסיסמתך התגלתה לגורם אחר, יש להחליפה מידית.

8. <u>שימוש במערכות המידע, בציוד לוגיסטי ובציוד המחשוב של רשות מקרקעי ישראל</u>

8.1. רשות מקרקעי ישראל מעמידה לרשות עובדיה מערכות מידע, ציוד לוגיסטי וציוד מחשוב, לצורך מילוי תפקידם, תקשורת שוטפת ועוד.

8.2. השימוש במערכות המידע, בציוד לוגיסטי ובציוד מחשוב, יבוצע לצרכי עבודה בלבד ובהתאם לתפקיד המוטל עליך.

8.3. חל איסור מוחלט על התקנת חומרה/ תוכנה מכל סוג שהוא ו/ או שינוי תצורת חומרה/ תוכנה הקיימת במחשבי הרשות לרבות מצעים נתיקים וציוד היקפי.

8.4. אם הנך עוזב את עמדת העבודה לפרק זמן קצר, עליך לנעול את המחשב.

8.5. בסיום יום עבודה, יש לוודא נעילת לוח המקשים (Ctrl+Alt+Delete או Win+L).

8.6. במידה ואתה עובד על מחשב ציבורי (המיועד לשימוש רב משתמשים), נדרש לבצע Log Off בסיום העבודה על המחשב.

8.7. עליך לבצע שימוש מושכל בהתאם למשאבי הרשת והאחסון ברשת. שימוש מוגזם עלול לפגוע בזמינות הרשת ובמערכות המידע.

8.8. עם סיום עבודתך ברשות, עליך להחזיר את כלל הציוד הלוגיסטי וציוד המחשוב אותו קיבלת בתחילת ובמהלך עבודתך. ראה נוהל סיום עבודה ... (סגירת יוזר, החזרת תג, מחיקת הרשאות)

9. <u>שימוש בהתקן אחסון נייד (Disk on key) לעובדים המורשים לכך</u>

9.1. אין לעשות שימוש בהתקני אחסון ניידים ברשות למעט עובדים שקיבלו הרשאה מיוחדת לשימוש בהתקן אחסון נייד והונפקו להם התקנים ייעודיים ומאובטחים לצורך כך.

9.2. על בעלי התפקידים ברשות מקרקעי ישראל, אשר סופק להם אמצעי זיכרון חיצוני/נתיק, חל איסור מוחלט לעשות כל שימוש באמצעי זה שלא לצרכי עבודה ו/או שלא באמצעי המחשוב של הרשות.

9.3. אין להעביר אמצעי זיכרון נתיק לבעל תפקיד אחר ללא העברת חתימות על טופס "קבלת ציוד" וטופס "אחריות אישית" באופן מסודר מול נציג צוות הפעלה/אמרכלות.

9.4. שימוש במכשירי טלפון חכמים (Smart Phones) כאמצעי זיכרון נתיק אסורה. איסור זה מתייחס גם למכשירי טלפון חכמים, אשר סופקו לבעלי התפקידים על ידי הארגון. סעיף זה כולל גם צילום מסך המחשב באמצעות הטלפון החכם ושליחתו.

9.5. יש לשמור על התקן האחסון הנייד מפני שימוש על ידי גורם שאינו מורשה.

9.6. עליך לנקוט בכל אמצעי הזהירות הסבירים על מנת לא לאבד ו/ או לגרום נזק להתקן האחסון הנייד שברשותך. במידה וההתקן הנייד אבד יש לדווח מידית למנהל הגנת הסייבר ברשות.

9.7. בכל חיבור של התקן זיכרון חיצוני לאמצעי מחשוב של רשות מקרקעי ישראל, עליך לבצע סריקה יזומה של ההתקן בעמדת הלבנה ייעודית הנמצאת בדלפק סיוע ו/או אצל צוות הפעלה.

9.8. אם הנך חושד לקיום קוד זדוני על גבי אמצעי הזיכרון הנתיק ו/או תפקוד לקוי של ההתקן, עליך להודיע על כך למנהל הגנת הסייבר ולבצע מחיקה כוללת של המידע שעל ההתקן (Format).

9.9. בגמר השימוש באמצעי הזיכרון הנתיק, יש להקפיד ולמחוק ממנו את הקבצים המכילים מידע פנימי ו/או חסוי/חסוי אישי/ ו/או חסוי ביותר של רשות מקרקעי ישראל.

10. <u>נשיאת מידע על גבי רכיבי מחשוב ניידים ומצעים נתיקים</u>

10.1. עליך לשמור כל מידע הנדרש לצורך עבודתך אך ורק במערכות המידע או בכונני הרשת של הרשות. <u>חל איסור</u> לשמור מידע על גבי רכיבי מחשוב ניידים/ מצעים נתיקים, אלא אם קיבלת אישור מפורש לכך.

10.2. חל איסור על שימוש ברכיבי מחשוב ניידים/אמצעי צילום אחרים לצורך צילום מידע שאינו כללי, אלא אם קיבלת אישור מפורש לכך.

10.3. בעת טיסה או נסיעה בכלי תחבורה ציבורי, רכיבי המחשוב הניידים/ המצעים הנתיקים יהיו אתך בתא הנוסעים ולא יאוחסנו יחד עם הכבודה בתא המטען.

10.4. אין להשאיר את רכיבי המחשוב הניידים/ המצעים הנתיקים ללא השגחה.

10.5. אם הנך חושד כי גורם לא מורשה ביצע שימוש ברכיבי מחשוב ניידים/ מצעים נתיקים, עליך לבצע את הפעולות הבאות:

10.5.1. להודיע על כך מידית למנהל הישיר ולמנהל הגנת הסייבר.

10.5.2. לאפס את סיסמת הגישה לרשת, עצמאית או באמצעות פנייה לדלפק הסיוע.

10.5.3. לא להשתמש ברכיבים אלו עד לסיום בדיקתם וקבלת אישור מצוות אב"מ.

11. <u>עבודה מרחוק לעובדים המורשים לכך</u>

11.1. ההרשאה לחיבור מאובטח SSL VPN שניתנה לך, הינה לשימושך האישי בלבד ואינך רשאי לתת לגורם אחר להשתמש בה.

11.2. אין להשאיר מחשב נייד/ נייח מחובר מרחוק לרשת הרשות, פתוח וללא השגחה.

11.3. בשימוש במחשב נייד של הרשות, אין אישור לשמור מידע מקומית (כונן C), אלא על גבי תיקיות רשת בלבד.

11.4. חל איסור לשמור כל מידע על גבי מחשב פרטי.

12. <u>שימוש בדואר אלקטרוני</u>

12.1. הדואר האלקטרוני הארגוני מהווה כלי עבודה, הנועד לשמש אותך לביצוע פעילות שוטפת במסגרת תפקידך. אין לעשות בו כל שימוש שלא למטרות עבודה ו/או שימוש העלול לסכן את מערך המחשבים והמידע של הארגון.

12.2. חל איסור מוחלט לשליחה, קבלה ו/או שמירת כל מידע פרטי בתיבת הדואר של רשות מקרקעי ישראל אשר אין לו זיקה לעיסוקך המקצועי ולהגדרות התפקיד שלך.

12.3. כל שימוש בדואר אלקטרוני ייעשה תוך ציות לכללים אלה, שמירה על לשון החוק ולפי הוראות הדין.

12.4. אין לפתוח הודעות דואר אלקטרוני ו/או לאשר קבלת קבצים המצורפים להודעות אלה ו/או ללחוץ על קישור לכתובת מחוץ לארגון (הסכמה לקבלת קובץ מצורף – הודעה המתקבלת בצד הנמען מממשל זמין בעת זיהוי צרופה בהודעת דואר אלקטרוני אשר מקורם בכתובת בלתי מזוהה, לא אמינה ו/או לא מוכרת למשתמש).

12.5. עם פתיחת הודעת דואר נכנס, עליך לוודא כי לא קיימות התראות אודות איתור וירוס/ פוגען/ קוד זדוני על ידי מערכת האנטי וירוס, המותקנת בתחנת העבודה ו/או בשרתי הדואר הארגוני. עליך לשים לב להופעת התראות בחלונות קופצים, הודעות אוטומטיות במייל אודות איתור וירוס והודעות פרטניות מצוות אב"מ בנושא זה.

12.6. במידה ודבר דואר, המכיל קובץ מצורף, לא התקבל עקב חסימתו במערכות הגנת הסייבר ארגוניות, הנך 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 גורמי הגנת הסייבר של הרשות. במידה ומדובר בקובץ מסוג שנאסר לקבלה/שמירה/הפעלה, לא יתאפשר שחרור קובץ זה ותבוצע מחיקתו על ידי צוות טכנולוגיות/ דלפק סיוע.

12.7. במקרים של קבלת קבצי Microsoft Office באמצעות הדואר האלקטרוני מכתובות דואר חיצוניות לארגון, אין לאפשר הפעלת פקודות מאקרו, אלא אם כן קיים אישור מפורש ובכתב לכך מצד ראש תחום טכנולוגיות וגורם הגנת הסייבר.

12.8. חל איסור מוחלט על שליחת דואר אלקטרוני, המכיל כל סוג של מידע שאינו מוגדר ככללי, בין אם בגוף ההודעה ובין אם בצרופה, לכל גורם בלתי מורשה בתוך או מחוץ לארגון.

12.9. חל איסור מוחלט להעביר מידע לגורמים מחוץ לארגון, לרבות גורמים מורשים, המוגדר כרגיש מבחינת הארגון, מבחינת לקוחותיו 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.

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

12.11. אין לצרף להודעות דואר יוצא אל מחוץ לארגון, קבצים אשר נפחם עולה על 30MB. לנמענים בתוך הארגון, ובדגש על שליחה לרשימות תפוצה ,יש להימנע משליחת קבצים כצרופות, אשר נפחם עולה על 3Mb, אלא לשלוח קישור (Link) לקובץ.

12.12. עליך 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.

12.13. שם המשתמש, כתובת הדואר האלקטרוני והמידע הכלול במסרים אלקטרוניים או הודעות חייבים לשקף את המחבר בפועל של המסרים או ההודעות.

12.14. חל איסור על קריאה, לקיחה או חשיפה של תקשורת אלקטרונית של עובד אחר ללא רשות מאותו עובד.

12.15. חל איסור על העברת דואר אלקטרוני באופן אוטומטי (עקוב אחרי) לדואר אלקטרוני מחוץ לרשות.

13. <u>שימוש באינטרנט ברשות מקרקעי ישראל</u>

13.1. האינטרנט מסייע לעבודה, אך יש בו גם סכנה. עליך להיות ערני ומודע לאיומי הסייבר, אפילו בעת גלישה שגרתית באינטרנט.

13.2. אין ללחוץ על קישורים המגיעים ממקור לא מהימן.

13.3. מידע פנימי של הארגון, המועבר באינטרנט, חשוף לעיניים זרות – אין להעבירו בלא אישור הגורם המוסמך בארגון.

13.4. שימוש בלתי חוקי ברשת האינטרנט, עלול לחשוף את רשות מקרקעי ישראל לסיכונים, על כל ההיבטים הנובעים מכך (כולל חשיפה לתביעות משפטיות). על כן, אין לבצע פעילות ברשת האינטרנט אשר נוגדת את האינטרסים של הרשות ו/ או הנוגדת את החוק והוראות כל דין.

13.5. רשתות חברתיות מהוות סוג של קהילה המאפשרות החלפת מידע ושיתופו. בשימוש ברשתות אלה קיים סיכון לדליפת מידע חסוי אשר עלול לפגוע ברשות. על כן, יש לעשות שימוש זהיר באתרים אלו ולחלקם אף חסומה הגישה. אין לשתף מידע עסקי מסווג או כל מידע אחר של הרשות ברשתות אלו בחיבור מהבית או בכלל.

13.6. אין לחשוף מידע אודות רשות מקרקעי ישראל ולקוחותיה בעת השימוש באינטרנט כגון בבלוגים, בקבוצות דיון (News Group) וצ'טים (Chats).

13.7. חל איסור לפרסום באתרי אינטרנט מידע (מכל סוג) אשר שייך במישרין או בעקיפין לרשות מקרקעי ישראל.

14. <u>דיווח על אירועי אבטחת מידע</u>

14.1. בעת התרחשות אחד מהאירועים הבאים עליך להודיע עליו למנהלך הישיר ו/או לדלפק הסיוע ו/או מנהל הגנת הסייבר:

14.1.1. אובדן מידע (טלפון חכם שמותקנת עליו אפליקציית Boxer , מחשב נייד, דיסק, קובץ מסמכים וכדומה).

14.1.2. אירוע וירוס במחשב אישי.

14.1.3. חשד שעובד אחר מבצע עבירה משמעתית או פלילית בנוגע לגילוי סודות או למסירת מידע שלא כדין.

14.1.4. פרצה או חשיפת מידע כלפי חוץ.

14.1.5. כל חשד לאירוע אבטחתי בארגון.

14.2. הערנות ושיקול הדעת שלך, חשובים מכל מנגנון אבטחה.

ג. נספחים

15. 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 קשיח (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: _____

נספח ב' - טופס בקשה להעברת מידע רציפה

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_____

_____

אמצעי ההעברה

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

☐ אחר:_____

העברה בגין

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

☐ אחר:_____

פרטי מבצע ההעברה בפועל

שם ומשפחה:_____

טלפון: _____

<u>אישורים</u>

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