		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנה בסייבר
1.0	מהדורה	פרק א-8	ניהול נכסי מידע
	בתוקף מ	שם הנוהל	ניהול נכסי מידע
עמוד - 0 - מתוך 16	סיווג - פנימי	מספר	נוהל א8 (א)



ניהול נכסי מידע

תאריך	חתימה	תפקיד	שם ומשפחה	גרסה מס'
31.04.2016		יועצת אבטחת מידע 2hsecure	רונית חייפץ	1.0
01.04.2018		אבטחת מידע	נחום צור	1.0
10.10.2018		אחראי מערכות מידע ומיקור חוץ	מיכאל פרידמן	1.0

מעקב שינויים

תאריך	תיאור השינוי	תפקיד	מבצע השינוי	סוג שינוי	מס'

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


תוכן עניינים



רשות מקרקעי ישראל – נהלי הגנה בסייבר

1.0		מהדורה	הגנת הסייבר	תחום
		בתוקף מ	ניהול נכסים	פרק א-6
		סיווג - פנימי	ניהול נכסים	שם הנוהל
16	עמוד - 1 - מתוך 16		נוהל א8 (א)	מספר

א.	מבוא	- 3 -
1.	מטרה	- 3 -
2.	מסמכים ישימים	- 3 -
3.	הגדרות	- 3 -
4.	תחולה	- 4 -
5.	אחריות	- 4 -
ב.	שיטה	- 5 -
6.	רשומות מצאי נכסים	- 5 -
7.	בעלות על הנכסים	- 6 -
8.	שימוש קביל בנכסים	- 7 -
9.	החזרת נכסים	- 8 -
10.	תהליך סיווג המידע	- 8 -
11.	סימון מידע מסווג	- 12 -
נספחים		- 13 -
12.	נספח א' - שאלות לגזירת רמת הסיכון של המערכת	- 13 -

		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	פרק א-6	ניהול נכסים
	בתוקף מ	שם הנוהל	ניהול נכסים
עמוד - 2 - מתוך 16	סיווג - פנימי	מספר	נוהל א8 (א)

מבוא

1. מטרה

- 1.1. יצירת מסגרת לניהול נכסי המידע והתוויית כללי סיווג המידע ברשות מקרקעי ישראל (להלן: "הרשות" ו/או "רמ"י).
- 1.2. להבטיח כי כל נכסי המידע של הרשות נמצאים בביקוח וקיים גורם הנושא באחריות לגבי כל אחד מהנכסים.
- 1.3. קביעת עקרונות לגבי סיווג המידע ומערכות המחשוב המעבדות ומאחסנות אותו על מנת להבטיח כי נכסי המידע של הרשות יאובטחו ברמה הנדרשת.

2. מסמכים ישימים

- 2.1. מצאי נכסים
- 2.2. מסמך התאמת אמצעי אבטחה בהתאם לסיווג מערכות
- 2.3. נוהל א8.2.1 (א) - אבטחת אמצעי מחשוב ניידים
- 2.4. מדיניות להגנת הסייבר בממשלה
- 2.5. טופס טיולים

3. הגדרות

- 3.1. **בעל נכס מידע** - האחראי על המידע, על שינויו ו/או ההשפעה אשר תהיה לאובדנו על הפעילות הארגונית של הרשות.
- 3.2. **מערכת מידע** - מערכת טכנולוגית אשר בה נאגר, מעובד או מועבר מידע כמוגדר לעיל.
- 3.3. **מידע** - אוסף של נתונים בעלי משמעות האגורים במכלול סוגי המדיה, ובכלל זה נתונים האגורים במערכות המחשוב (שרתים, מחשבים אישיים ואמצעי מכשור ניידים אחרים) ונתונים האגורים על גבי מדיה מגנטית, אופטית, מידע מודפס וכו'.
- 3.4. **מאגר מידע** - מקבץ נתונים המאוחסן באמצעי ממוחשב.
- 3.5. **מצאי** - מונח לוגיסטי המקביל למונח נכס.
- 3.6. **משתמש** - בעל תפקיד הרשות או גורם חיצוני, אשר במסגרת תפקידו משתמש במערכות מידע.
- 3.7. **נכס מידע** - מערכת מידע או מצע פיזי האגורים מידע בעל ערך לרשות או מאגר מידע כמוגדר בחוק הגנת הפרטיות. ההתייחסות בנוהל זה היא רק לנכסי המידע הנמצאים בבעלות הרשות ומבוקרים על ידו.
- 3.8. **סיווג מידע** - הגדרת ערך יחסית לפגיעה שתיווצר לרשות אם מידע מסווג יגיע לידי גורם בלתי מורשה.


		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	פרק א-6	ניהול נכסים
	בתוקף מ	שם הנוהל	ניהול נכסים
עמוד - 3 - מתוך 16	סיווג - פנימי	מספר	נוהל א8 (א)

4. תחולה

4.1. הנוהל חל על כל בעלי התפקידים ברשות מקרקעי ישראל.

5. אחריות

5.1. יישום נוהל זה הינו באחריות כלל גורמי ההנהלה ובעלי התפקידים המוגדרים ברשות מקרקעי ישראל.

		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	פרק א-6	ניהול נכסים
	בתוקף מ	שם הנוהל	ניהול נכסים
עמוד - 4 - מתוך 16	סיווג - פנימי	מספר	נוהל 8א (א)

שיטה

6. רשומות מצאי נכסים

- 6.1. בשלב הראשון יבוצע זיהוי ומיפוי נכסי מידע ברשות ע"י בחינת המידע שמכיל כל נכס והתשתיות/ המערכות בהן הנכס משתמש ואשר מתממשקות אליו.
- 6.2. בשלב השני תבוצע הערכת רגישות הנכסים שמופו כפועל יוצא של הנזק הפוטנציאלי לרשות מפגיעה בכל אחד מהנכסים הללו.
- 6.3. בכל עת בה מתרחשים שינויים טכנולוגיים, שינויים בחוקים או רגולציות או שינויים ארגוניים, תבוצע הערכה מחודשת של הנכסים המושפעים מאותם שינויים.
- 6.4. מנהל הגנת הסייבר ינהל רשימות אשר יכילו תיעוד של הנכסים הפיזיים- ציוד מחשבים, ציוד תקשורת, תוכנות צד ג', נכסי / מאגרי מידע ושירותים.
- 6.4.1. נכסי מידע
- 6.4.1.1. מידע האגור בכל אחד מסוגי המדיה- מאגרי מידע, נהלים ותקנים, מדריכים והוראות הפעלה, תהליכי עבודה, תהליכים עסקיים וכיו"ב.
- 6.4.1.2. נכסי מידע לוגיים- מערכות מידע, אפליקציות, כלי פיתוח, תוכנות וכיו"ב.
- 6.4.1.3. נכסי מידע פיזיים- חומרת מחשוב, חומרת תקשורת, מצעי מידע מגנטיים, ציוד טכני, מידע מודפס וכיו"ב.
- 6.5. המצאי יכלול בין היתר את הנתונים הבאים:
- 6.5.1. שם הנכס ;
- 6.5.2. הפלטפורמה של הנכס ;
- 6.5.3. תיאור הנכס ;
- 6.5.4. מיקום הנכס ;
- 6.5.5. בעל הנכס ;
- 6.5.6. סוג המידע בנכס ;
- 6.5.7. רמת סיווג המידע של הנכס ;
- 6.5.8. שלמות המידע (RPO) ;
- 6.5.9. רמת הסיבולת להשבתה (RTO) ;
- 6.5.10. רמת הסיכון של הנכס ;

		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	ניהול נכסים	פרק א-6
	בתוקף מ	ניהול נכסים	שם הנוהל
עמוד - 5 - מתוך 16	סיווג - פנימי	נוהל א8 (א)	מספר

6.6. באחריות מנהל הגנת הסייבר, לעדכן באופן שוטף ולסקור אחת לתקופה את רשימת נכסי מידע ומערכות המידע הארגוניות, על מנת לוודא את עדכניותן.

6.7. תחזוקת המצאי הינה באחריות מנהל הגנת הסייבר. על בעל הנכס לעדכן את מנהל הגנת הסייבר בכל שינוי או תוספת.

6.8. מצאי רשומות ניהול **תוכנות** (כולל כלי פיתוח) יכול פרטים על תוכנות כגון: תוכנות יישומיות, כלי פיתוח ותוכנות שנרכשו מצד שלישי. בנוסף, יש לתעד את מספר הסריאלי של הרישיון החוקי להתקנתם. באחריות תחום טכנולוגיות ליצור ולתחזק רשימה זו.

6.9. מצאי רשומות **שירותים** יכול את תיעוד המידע על ספקי השירותים כגון: תכולת ההתקשרות עם ספקי השירותים, נהלי ספקי השירותים, סוג ההסכם (SLA) והיחידות המושפעות מהשירות. באחריות תחום טכנולוגיות ליצור ולתחזק רשימה זו.

7. בעלות על הנכסים

7.1. אחריות מנהל הגנת הסייבר:

7.1.1. זיהוי רמת הסייבוג של הנכס.

7.1.2. הגדרה ויישום אמצעי הגנה מתאים כדי להבטיח את סודיות, תקינות, וזמינות נכס המידע.

7.2. אחריותו של בעל הנכס:

7.2.1. עדכון מנהל הגנת הסייבר אודות הנכס ו/או שינויים המבוצעים על הנכס.

7.2.2. אישור מתן הרשאת גישה לנכס.

7.3. באחריות בעל הנכס לוודא את תקינותו וקיום תנאי העבודה האופטימאליים לנכס הכוללים את כלל המשאבים הנדרשים לתפקודו התקין והמיטבי.

7.4. בעל הנכס אחראי על הנכס ולכן מתוקף תפקידו לשמור על תפקודו התקין של הנכס ולמנוע פגיעה כלשהי בנכס.

7.5. על בעל הנכס מוטלת האחריות לבקרה ויישום מדיניות הגנת הסייבר על הנכס לפי הגדרות ומדיניות הרשות.

7.6. בעל הנכס יעביר עדכונים שוטפים למנהל הגנת הסייבר לגבי ההתאמה בין מדיניות הגנת הסייבר ליישומו בפועל.

7.7. מטרת בעל הנכס תהיה ליצור מצב של שיפור מתמיד ברמת הגנת הסייבר. כנגזרת מכך, בעל הנכס יעדכן על כל אירוע סייבר אשר יתרחש במסגרת הנכס.


7.8. בעל הנכס אמון על מיקומו, אבטחתו הפיזית ותיעוד הפרטים הרלוונטיים לאבטחתו.

		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	ניהול נכסים	פרק א-6
	בתוקף מ	ניהול נכסים	שם הנוהל
עמוד - 6 - מתוך 16	סיווג - פנימי	נוהל 8א (א)	מספר

7.9. בעל הנכס יוודא שימוש תקין וראוי בנכס וימנע חריגות.

8. שימוש קביל בנכסים

- 8.1. על בעל תפקיד ברשות לעשות שימוש בנכסי המידע כמקובל ברשות מקרקעי ישראל.
- 8.2. מנהל הגנת הסייבר יגדיר את ההנחיות לשימוש מאובטח בציוד על ידי בעלי התפקיד ברשות.
- 8.3. ההנחיות יופצו לבעלי התפקיד ברשות בהתאם לרלוונטיות, לרבות הפצתן של הוראות הפעלה טכניות של מערכות לוגיות ופיזיות, רכיבי או מנגנוני הגנה, מחשבים ניידים וכיו"ב.
- 8.4. באחריות צוות שטח והדרכה, בתיאום עם בעלי התפקידים הרלוונטיים, לגבש נהלים והנחיות לשימוש במערכות המידע ברשות. כמו כן, עליהם להדריך את בעלי התפקידים על אופן השימוש במערכות המידע ברשות ולעדכןם כאשר מתבצעים שינויים במערכות המידע.
- 8.5. שימוש בלתי קביל בנכסי המידע חושף את הרשות לסיכונים כמו נזקות, נזק לנכסים, תביעות משפטיות וכיו"ב.
- 8.6. כלל נכסי המידע אשר נמצאים בבעלות רשות מקרקעי ישראל נועדו לשרת את מטרותיה העסקיות בלבד, והם קניינה של הרשות. בהתאם לכך, הרשות יכולה לגשת, לבקר, לנטר, להעתיק, לחסום ולמחוק הרשאות משתמש מסיבות עסקיות.
- 8.7. יתר על כן, רשות מקרקעי ישראל עשויה לחשוף תקשורת של משתמש עם גורם שלישי, לכן על המשתמש לא לעשות שימוש פרטי בדוא"ל ובכל תקשורת העוברת ברשת של רשות מקרקעי ישראל.
- 8.8. כל נכס הנמצא בבעלות רשות מקרקעי ישראל, כגון דיסקים, אמצעי אחסון ניידים, מסמכים, קבצים וכיו"ב יכולים להיבדק ע"י הרשות בכל עת, עם או ללא הודעה או הסכמה מוקדמת.
- 8.9. הפרה של ככלי השימוש בנכסים ע"י בעלי תפקיד ברשות, עשויה לגרום לנקיטת צעדים משמעותיים, עד לכדי סיום העסקה. הפרה של הכללים ע"י עובד זמני, קבלן או ספק עלולה לגרום לסיום החוזה שלהם.
- 8.10. חל איסור מפורש על שימוש בנכסי הרשות לכל אחת מהמטרות הבאות:
 - 8.10.1. עיסוק בפלילים.
 - 8.10.2. פעילות בלתי מורשית להשגת כסף או הפעלת עסק פרטי.
 - 8.10.3. הפצת מכתבי שרשרת, דואר זבל או התכתבות דומה.
 - 8.10.4. העברת מסרים מטרידים.
 - 8.10.5. הפצה, צפייה, הורדה, אחסון, העברה וכיו"ב של תכנים נושאי אופי מיני או מידע אחר העשוי להוות עלבון או לגרום להשפלה, אפליה, ביזוי, הטרדה של בעל תפקיד כלשהו.
 - 8.10.6. הורדה או אחסון של מידע ו/או תוכנה המוגנים בזכויות יוצרים וללא רישיון עסקי.

		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	ניהול נכסים	פרק א-6
	בתוקף מ	ניהול נכסים	שם הנוהל
עמוד - 7 - מתוך 16	סיווג - פנימי	נוהל 8א (א)	מספר


9. החזרת נכסים

- 9.1 בעל תפקיד אחראי לכל הרכוש והחומר הכתוב שהונפקו לו או היו בחזקתו במהלך עבודתו ברשות.
- 9.2 עם סיום העבודה, על בעל התפקיד להחזיר את כל הציוד שניתן לו על ידי הרשות במהלך עבודתו. חפצים אלו כוללים בין השאר: מחשב נייד, תוכנה, נתונים, תיעוד, חוברות הדרכה, מסמכים וכדומה, בהתאם לרשימת רשימת הציוד עליו חתם בעל התפקיד.
- 9.3 באחריות האמרכלות לוודא החתמת טופס סיום העסקה על ידי כל הגורמים הרלוונטיים ברשות.
- 9.4 בעל תפקיד יגיע פיזית לדלפק הסיוע להחזרת כל הציוד שברשותו, כפי שרשום על שמו, במסגרת טופס סיום העסקה.
- 9.5 באם בעל תפקיד לא מחזיר את הציוד (כולו או חלקו), על מנהל דלפק הסיוע לידע את מנהלו הישיר של בעל התפקיד והטיפול יועבר לאחריותו תוך עדכון ראש תחום הגנת סייבר.

10. תהליך סיווג המידע

10.1 עקרונות לסיווג מידע

- 10.1.1 סיווג המידע מתייחס לכל מצע או מאגר בהם קיים המידע (קבצים, בסיסי נתונים, אמצעי מדיה אלקטרונית או אופטית, מסמכים וכיו"ב).
- 10.1.2 סיווגו של המידע יקבע בהתאם לרמת הרגישות הגבוהה ביותר הקיימת בקובץ, במאגר או במצע הפיזי בהם אגור המידע (על פי עקרון "המחמיר קובע").
- 10.1.3 סיווג המידע יוביל לסיווג מערכת המידע, כלומר מערכת המידע תסווג בהתאם למידע המועבד באמצעותה.
- 10.1.4 סיווג מערכות מידע ויישומים יוביל להגדרת רמת ההגנה הנדרשת, תוך התייחסות לרמת ההזדהות, רמת המידור, רמת הבקרה, צורך בהצפנה וכיו"ב.
- 10.1.5 סיווג של מערכת חדשה יתבצע עוד בשלב אפיון המערכת, על מנת לאפשר את שילובם של אמצעי ההגנה הנדרשים בשלב הפיתוח.
- 10.1.6 רמות הסיווג יתוו את דרכי הטיפול במידע ויתבססו על הסיכונים הפוטנציאליים הרלוונטיים לרשות והמוגדרים באופן דינאמי במסגרת ביצוע סקרי הסיכונים המתקיימים ברשות.
- 10.1.7 רמת ההגנה המחייבת את יוצרי המידע, מאגריו ומערכותיו תיקבע ע"י מנהל הגנת הסייבר ברשות ובאישור ועדת היגוי לנושאי הגנת הסייבר.
- 10.1.8 רמת ההגנה תקיף ותכסה את המידע על כל התחומים הנגזרים ממנו (אבטחה פיזית, אבטחת רשומות, הגנה לוגית, אבטחת מהימנות עובדים והגנת ממשקים עסקיים).

		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	פרק א-6	ניהול נכסים
	בתוקף מ	שם הנוהל	ניהול נכסים
עמוד - 8 - מתוך 16	סיווג - פנימי	מספר	נוהל א8 (א)

10.1.9. רמת הגנת המידע בכל המערכות ומתקני הרשות לא תהיה פחותה מרמת ההגנה המחייבת הנמוכה ביותר שתקבע.

10.2. רמות סיווג מידע

10.2.1. קביעת עקרונות לרמות סיווג של המידע תיעשה עפ"י הנזק הצפוי לרשות במקרה של פגיעה באמינות, בזמינות או בחסיון המידע.

10.2.2. סוגי המידע הקיימים ברשות (אחד או יותר):

10.2.2.1. מידע בטחוני.

10.2.2.2. מידע אישי מוגן פרטיות על פי חוק הגנת הפרטיות- התשמ"א 1981.

10.2.2.3. מידע כלכלי ו/או מסחרי.

10.2.2.4. מידע אודות מדיניות ציבורית בהתהוות.

10.2.2.5. מידע שקיים לגביו חיסיון על פי חוק.

10.2.2.6. מידע הנוגע לשלום הציבור ו/או לשלום היחיד.

10.2.2.7. מידע על ניהולה התקין של הרשות.


10.2.3. רמות הסיווג למידע שאינו בטחוני יהיו בהתאם לארבעת הרמות הבאות:

10.2.3.1. **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.

10.2.3.2. **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.

10.2.3.3. **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.

10.2.3.4. **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.

		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	פרק א-6	ניהול נכסים
	בתוקף מ	שם הנוהל	ניהול נכסים
עמוד - 9 - מתוך 16	סיווג - פנימי	מספר	נוהל א8 (א)

10.2.4. סיווג מידע בטחוני יעשה לפי הנחיות הרשות הממלכתית לאבטחת מידע ובהתאם להנחיות גופי הביטחון השונים אשר לרשות קשר עימם בהתאם ל- 4 רמות סיווג:

10.2.4.1. בלמ"ס

10.2.4.2. שמור

10.2.4.3. סודי

10.2.4.4. סודי ביותר

10.3. טיפול במידע

הטיפול במידע יתבצע בהתאם לסיווגו כמפורט בסעיף 10.2.3 בנוהל זה.

10.4. פרמטרים לקביעת סיווג המידע

10.4.1. טרם קביעת סיווגו של נכס מידע או מערכת מידע, יש לשקול את מידת השפעתם או מידת הרלוונטיות של הפרמטרים הבאים. ככל שמידת ההשפעה או הרלוונטיות גבוהות יותר, כך ניתן להסיק כי המידע רגיש יותר ויש לסווגו ברמת סיווג גבוהה יותר.

10.4.1.1. **מידת הנזק** - מידת הנזק שייגרם לרשות ו/או ללקוחותיה ו/או לבעלי תפקיד, במידה והמידע יפגע ו/או יגיע לגורמים בלתי מורשים.

10.4.1.2. **מחויבות חוקית** - פגיעה פוטנציאלית בלקוחות ו/או בעלי תפקיד ברשות משום הפרת מחויבות חוקית כלפי חוק הגנת הפרטיות התשמ"א - 1981. אפשרות זו נובעת לרוב מסיווג מידע לקוי והמשך טיפול בלתי הולם במידע, נסיבות המגדילות את אפשרות הפגיעה במידע ו/או הגעתו של מידע לידי גורמים בלתי מורשים.

10.4.1.3. **עיתוי** - רמת הרגישות עשויה להשתנות על ציר הזמן. נכס מידע יישא רמת רגישות גבוהה ביותר עד לרגע פרסומו והפיכתו לנחלת הכלל (לדוגמא, מבצע שיווקי יהיה רגיש יותר עד פרסומו ולכן סיווגו של המידע יהיה גבוה יותר עד לשלב זה. כמו כן, תכנית כלכלית תהיה רגישה יותר עד למועד יישומה והוצאתה לפועל).

10.4.1.4. **רמת פירוט** - ככל שרמת פירוט הנתונים גבוהה יותר, כך לרוב תהיה רמת רגישות המידע גבוהה יותר ומידת הנזק גדולה יותר, היה והמידע יגיע לגורמים בלתי מורשים (לדוגמא: קובץ מפורט המכיל את מספרי תעודת הזהות, כתובותיהם, מספרי הטלפון, מצבם המשפחתי, תאריכי הלידה ונתוני השכר של העובדים, יהיה רגיש יותר מאשר קובץ הכולל את מספרי תעודת הזהות בלבד).

10.4.1.5. **כמות** - ככל שכמות המידע המצוי במערכת מידע גדולה יותר, כך הינו רגיש יותר ומידת הנזק עלולה להיות גדולה יותר, במידה והמידע יגיע לגורמים בלתי מורשים (לדוגמא: קובץ המכיל את

		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	פרק א-6	ניהול נכסים
	בתוקף מ	שם הנהל	ניהול נכסים
עמוד - 10 - מתוך 16	סיווג - פנימי	מספר	נוהל א8 (א)

כלל הלקוחות של הרשות, להם זכויות בנכסים/קרקע, יהיה רגיש יותר ומסווג ברמה גבוהה יותר מאשר זה המכיל רק מספר מצומצם של לקוחות).

10.5 שיטה לסיווג נכסי מידע

10.5.1 כלל נכסי המידע בארגון ימופו לתוך טבלת אקסל.

10.5.2 הטבלה תכיל נתונים טכניים הנוגעים במערכת כגון:

10.5.2.1 למה משמשת המערכת?

10.5.2.2 איזה סוג מידע מכילה?

10.5.2.3 סיווג המידע?

10.5.2.4 כמה משתמשים יש בה?

10.5.2.5 האם המערכת היא בעלת ממשקים למערכות אחרות או לאינטרנט?

10.5.2.6 בעל המידע (תפקיד)

10.5.2.7 האם נתמכת ע"י ספק חיצוני ע"י חיבור מרחוק ?

10.5.2.8 האם נתונים מסווגים מוצפנים?

10.5.3 הטבלה תכיל מספר שאלות אשר מהן תיגזר רמת הסיכון של המערכת. השאלות יתמקדו בשלושת

המרכיבים של ה CIA :

10.5.3.1 סודיות

10.5.3.2 זמינות

10.5.3.3 אמינות

10.5.4 לרשימת שאלות בנושאים השונים ראה נספח א'.

10.5.5 טבלה זו תשמש את הרשות לצרכים הבאים :

10.5.5.1 קביעת רמת הסיכון של המערכות וגזירה, כתוצאה מכך, של רמת האבטחה אשר יש ליישם

במערכות אלו וכן תדירות הבדיקות (סקרי סיכונים ומבחני חדירה) במערכות אלו.

10.5.5.2 תכנון נכון של מערך ה-DRP שייקבע לפי רמת הזמינות הנדרשת מהמערכת.

10.5.6 איסוף מידע

10.5.6.1 בשלב ראשון יבוצעו ראיונות עם בעלי תפקידים רלוונטיים, במטרה ללמוד על תהליכי

העבודה, רגישות המידע והסביבות הטכנולוגיות השונות.

10.5.6.2 תהליך האיסוף יהווה למעשה את שלב המיפוי של נכסי המידע.

10.5.6.3 יתקיימו פגישות פרונטליות עם גורמי הנהלה ברמות בכירות שונות (ראשי צוותים, ראשי

תחומים, ראשי מחלקות וכו'). על מנת להשלים את הפער לגבי המידע בארגון, יתקיימו פגישות

		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	פרק א-6	ניהול נכסים
	בתוקף מ	שם הנוהל	ניהול נכסים
עמוד - 11 - מתוך 16	סיווג - פנימי	מספר	נוהל א8 (א)

נוספות עם גורמי הנהלה ואנשי מפתח באגפים ובחטיבות נוספות ברשות מקרקעי ישראל. להלן פירוט בעלי התפקידים בארגון המשמשים כגורמי מפתח בתהליך לימוד התהליכים, איסוף מידע ומיפוי.

10.5.7. רמות סיווג לנכסי המידע

10.5.7.1. שלב זה יתבצע בשיתוף עם גורמי הנהלה מאגף מערכות מידע ומחשוב ברשות מקרקעי ישראל, כאשר מפעילות זו ייגזרו ההמלצות מהמצאים שעלו בשלב הקודם.

10.5.7.2. הגדרת מנגנוני אבטחת מידע נחוצים לכל רמת סיווג, זאת בהתאם לרמות הסיכון, אליהן חשוף המידע ו/או המערכת.

10.5.7.3. הגדרת עקרונות הרשאת גישה למשתמשים בהתאם לעקרון "הצורך לדעת".

10.5.7.4. שיוך כלל נכסי מידע לרמת סיווג מתאימה.

10.5.7.5. הגדרת חוקיות/לוגיקה עבור מערכת אבטחת מידע, אשר נועדו להגן על נכסים ומערכות מידע ברמות סיווג שונות.

10.5.8. הגדרת רמת סיכון עבור נכסי ומערכות המידע

10.5.8.1. כחלק מתהליך המיפוי, הסיווג ומתן המענה האבטחתי המתאים לנכסי המידע ולמערכות המידע הארגוניות, יבוצע גם תהליך הערכת רמת הסיכון בו נמצאים המידע ו/או המערכת.

10.5.8.2. בתהליך זה ישוכללו כלל הנתונים הרלוונטיים הידועים על הנכס/ המערכת על מנת לקבוע את רמת הסיכון (כמפורט בנספח א').

10.5.8.3. לאחר מכן ישוכללו בקרות האבטחה המופעלות על הנכס/ מערכת (כמפורט בנספח א'), על מנת לקבוע את רמת הסיכון השיורי ואת הפעילות הנדרשת (בקרות מפצות) כפועל היוצא מכך.

10.5.8.4. תהליך זה יבוצע על פי הנורמות הרווחות בתחום, תוך התאמת המודל לצרכי הארגון.

10.6. **טיפול במערכות חדשות**


10.6.1. באחריות מנהל מערכות מידע להנחות את אגף מערכות מידע ומחשוב, כי כל מערכת חדשה המותקנת והנמצאת בשימוש של גורם כלשהו ברשות, בין אם מדובר במוצר מדף או במערכת בפיתוח עצמי, תעבור תהליך רישום וסיווג טרם תחילת השימוש בה.

10.6.2. סיווג המערכת יבוצע לפי הוראות נוהל זה.

11. סימון מידע מסווג

11.1. יש לציין באופן בולט וברור על כל פריט מידע את סיווגו ו/או את רמת רגישותו.

11.2. מסמכים המופקים ממערכות מידע ממוחשבות יסווגו ע"י המערכת עצמה באופן אוטומטי, אם מערכת המידע מאפשרת זאת.

		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	פרק א-6	ניהול נכסים
	בתוקף מ	שם הנוהל	ניהול נכסים
16	עמוד - 12 - מתוך 16	מספר	נוהל א8 (א)

ב. נספחים

12. נספח א'- שאלות לגזירת רמת הסיכון של המערכת

12.1. הסתברות לסיכון (כללית לשלושת הסיכונים)

מס'	השאלה	מטרת השאלה	הציון
1	כמה משתמשים יש במערכת?	ככל שיש יותר משתמשים קיים סיכון גדול יותר של פגיעה בשלמות הנתונים במערכת.	1- עד 50 2- 50-100 3- מעל 100
2	קשר למערכות אחרות- מספר הממשקים הפנימיים	ככל שיותר מערכות מסתמכות על הנתונים במערכת, כך חשיבות דיוק הנתונים במערכת עולה.	1- אין ממשקים למערכות אחרות 2- עד 5 ממשקים פנימיים 3- מעל 5 ממשקים פנימיים
3	קשר לגורמי חוץ- מספר הממשקים החיצוניים	ככל שיותר מערכות מסתמכות על הנתונים במערכת, כך חשיבות דיוק הנתונים במערכת עולה.	1- אין ממשקים למערכות אחרות 2- עד 3 ממשקים חיצוניים 3- מעל 3 ממשקים חיצוניים
4	גישה מרוחקת	מערכות החשופות לאינטרנט נמצאות ברמת סיכון גבוהה יותר לדליפה של נתונים- על כן יש להגדיר כי הן נמצאות ברמת סיכון גבוהה יותר	1- אין גישה מרוחקת למערכת 2- אתר אינטרנט 3- קיימת גישה מרוחקת למערכת
5	אופי תחזוקת המערכת	במידה והמערכת מתוחזקת באופן שוטף על ידי גורם חיצוני- עולה רמת הסיכון של המערכת לזליגת מידע	1- ניהול עצמי מקומי 2- ניהול עצמי מרחוק/ ניהול מקומי ע"י ספק חיצוני 3- ספק חיצוני מרחוק
6	מספר התומכים הטכנולוגיים	ככל שיש יותר תומכים טכנולוגיים למערכת, כך הסיכון לאמינות, זמינות וסודיות הנתונים במערכת עולה.	1- עד 5 2- בין 6-10 3- למעלה מ-10

12.2. סודיות

מס'	השאלה	מטרת השאלה	הציון
1	נכסי מידע/ סוג המידע במערכת	מערכת מוגדרת קריטית כאשר קיים חשש למידע רגיש/ מסווג.	1- לא 5- כן
2	כמות הנתונים במערכת	ככל שכמות הנתונים במערכת גדולה יותר, יש סיכון למידע רב יותר.	1- עשרות אלפי רשומות/ מגות 2- מאות אלפי רשומות/ גיגות 3- מיליוני רשומות/ טרות

12.3. זמינות

מס'	השאלה	מטרת השאלה	הציון
1	ערך/ קריטיות המידע	בהתאם לקריטיות של המערכת לארגון זמן ההעלאה לאוויר לאחר קריסה מתקצר.	1- RTO=מעל 4 ימים 2- RTO=בין 2-4 ימים 3- RTO=עד יומיים



רשות מקרקעי ישראל – נהלי הגנה בסייבר


		הגנת הסייבר	תחום
1.0	מהדורה	ניהול נכסים	פרק א-6
	בתוקף מ	ניהול נכסים	שם הנוהל
16	עמוד - 13 - מתוך	נוהל א8 (א)	מספר

12.4. אמינות

מס'	השאלה	מטרת השאלה	הציון
1	מרכזיות המערכת- האם מערכות אחרות מסתמכות על המידע המוחזק במערכת?	ככל שיותר מערכות מסתמכות על הנתונים במערכת, כך חשיבות דיוק הנתונים במערכת עולה.	1- מערכת קצה 2- מערכת ליבה- מערכות אחרות תלויות במערכת לשם קבלת נתונים 3- מערכת תשתיתית
2	כמות הפעולות הנעשות במערכת ביום	ככל שנעשה מספר רב יותר של פעולות ביום, עולה הסיכון לפגיה באמינות נתוני המערכת.	1- בודדות 2- עשרות 3- מאות עד אלפים

12.5. אפקטיביות בקרות

מס'	השאלה	הציון
1	אופן שמירת הנתונים	1- לא מוצפן 3- מוצפן
2	האם נעשה שימוש בסיסמאות מורכבות (6 תווים לפחות, אות גדולה, אות קטנה, אותיות ומספרים)?	1- לא. 5- כן.
3	האם קיים מנגנון להחלפת סיסמאות לאחר פרק זמן מוגדר (60 יום)?	1- לא. 5- כן.
4	האם מיושמת הזדהות אישית וחד ערכית למשתמשי ולמנהלי מערכת?	1- לא 2- רק למשתמשי מערכת. 3- למשתמשי מערכת ולמנהלי מערכת.
5	האם קיים מנגנון נעילה לאחר 5 נסיונות גישה כושלים?	1- לא.
6	האם מופעל מנגנון לניתוק Session לאחר לכל היותר 15 דק' של אי פעילות במערכת?	5- כן.
7	האם מוצפנות סיסמאות מורשי הגישה ליישום?	1- לא. 5- כן.
8	האם תווד התקשורת בתהליך ההזדהות מוצפן?	1- לא. 5- כן.
9	האם המשתמש מחוייב להחליף סיסמה בשימוש ראשון במערכת?	1- לא. 5- כן.
10	האם מיושם עיקרון 2 factor authentication בגישה מתוך הארגון ובגישה מרחוק?	1- לא 2- רק מחוץ לארגון 3- מתוך הארגון ומחוץ לארגון

		רשות מקרקעי ישראל – נהלי הגנה בסייבר	
		תחום	הגנת הסייבר
1.0	מהדורה	פרק א-6	ניהול נכסים
	בתוקף מ	שם הנוהל	ניהול נכסים
16	עמוד - 14 - מתוך 16	מספר	נוהל א8 (א)
	סיווג - פנימי		

11	האם הרשאות המערכת מנוהלות במערכת ניהול הרשאות?	1- לא. 5- כן.
12	האם מבוצע תיעוד (LOG) של הפעילויות הרגישות במערכת?	1- לא 2- חלקי 3- כן
13	האם מבוצע תיעוד (LOG) שינויים במערכת?	1- לא 2- חלקי 3- כן

- 12.6. מילוי ערכי התשובות לשאלונים במחשבון הערכת סיכונים יסייע בקביעת ערך לרמת הסיכון של המערכת.
- 12.7. על בסיס ניקוד השאלות, יחושב ערך ממוצע לכל היבט - זמינות, שלמות וחיסיון.
- 12.8. בכל מערכת תבוצע גם הערכת חשיבות של כל אחד מהיבטים אלה - משקולות.
- 12.9. אח"כ יבוצע ממוצע משוקלל המגדיר את רמת הסיכון השורשי במערכת.
- 12.10. לבסוף יש להחיל את אפקטיביות הבקורות על רמת הסיכון השורשי במערכת על מנת לקבל את הסיכון השיווי של המערכת.
- 12.11. השאלונים ימולאו באופן תקופתי, בכל פעם שתבוצע הערכת סיכונים.
- 12.12. הציון הסופי ישמש אמצעי להערכת רמת הסיכון ולהשוואת רמת הסיכון בין המערכות השונות.