אבטחת ספקים

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

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

רשות מקרקעי ישראל– נהלי הגנה בסייבר			
תחום	הגנה בסייבר		
פרק א-15	ארגון אבטחת מידע	מהדורה	1.0
שם הנוהל	**אבטחת ספקים חיצוניים**	בתוקף מ	
מספר	א-15	**סיווג** - פנימי	עמוד - 1 - מתוך 20

תוכן עניינים

א. מבוא ..... - 3 -

1. כללי ..... - 3 -

2. מטרה ..... - 3 -

3. מסמכים ישימים ..... - 3 -

4. הגדרות ..... - 4 -

5. אחריות ..... - 4 -

6. תחולה ..... - 5 -

ב. שיטה ..... - 6 -

7. הקשרות עם ספק ..... - 9 -

8. שילוב פרק אבטחת מידע בהקשרות עם ספק ..... - 9 -

9. התחייבות לשמירה על סודיות המידע במסגרת התקשרות עם ספקים חיצוניים ..... - 9 -

10. ליווי פעילות עובדים במסגרת התקשרות עם ספקים חיצוניים ..... - 9 -

11. הקמת חשבון משתמש במסגרת התקשרות עם ספקים חיצוניים ..... - 10 -

12. מתן הרשאות גישה במסגרת התקשרות עם ספקים חיצוניים ..... - 10 -

13. גישה מרחוק למערכות המחשוב במסגרת התקשרות עם ספקים חיצוניים ..... - 10 -

14. אבטחת תווך התקשורת במסגרת התקשרות עם ספקים חיצוניים ..... - 11 -

15. פעילות בקרה במסגרת התקשרות עם ספקים חיצוניים ..... - 11 -

16. הערכה וטיפול בחשיפות אבטחה ..... - 13 -

17. סיום התקשרות עם ספקים ..... - 13 -

נספחים ..... - 14 -

18. נספח א'- שאלון לבדיקת הגנת סייבר בחצרות הספק ..... - 14 -

19. נספח ב'- התחייבות לשמירה על סודיות ..... - 15 -

20. נספח ג' – התחייבות לשמירה על סודיות חשכ"ל ..... - 18 -

א. מבוא

1. כללי

המידע האגור במאגרי המידע ובמערכות המידע של רשות מקרקעי ישראל הנו משאב קריטי, עיקרי ובעל ערך מהותי לפעילות השוטפת של הרשות ולמילוי ייעודה ותפקידה כמשרד ממשלתי.
על כן, על הרשות להגן על נכסי המידע שלה, ולפעול למניעת שיבוש המידע בהם ושימוש לא ראוי בהם .

2. מטרה

2.1 להפחית את הסיכונים הנובעים מהעבודה עם ספקים חיצוניים.

2.2 להבטיח כי ספקים חיצוניים של רשות מקרקעי ישראל פועלים בהתאם למדיניות הגנת הסייבר של הארגון.

2.3 הגדרת תהליך מסודר להתקשרות ועבודה עם ספקים חיצוניים ובכך למזער את הסתברות מימוש הסיכונים, הנובעים מתצורת פעילות זו.

2.4 הגדרת מסגרת דרישות סף ובקרות, באמצעותן ניתן יהיה להבטיח כי ספקים חיצוניים של רשות מקרקעי ישראל פועלים בהתאם למדיניות הגנת הסייבר של הארגון .

3 מסמכים ישימים

3.1 מתודולוגיה לניהול סיכוני הגנת הסייבר.

3.2 א-8 ניהול נכסים.

3.3 א-9 בקרת גישה.

3.4 א-13 אבטחת תקשורת.

3.5 א-18 תאימות ומאגרי מידע

3.6 הסכם התקשרות.

3.7 כתב התחייבות לשמירה על סודיות

3.8 חוק הגנת הפרטיות התשמ"א-1981

3.9 הנחית רשם מאגרי מידע מס' 2/2011שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי.

4 הגדרות

4.1 **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.

4.2 **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.

4.3 **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.

4.4 **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.

4.5 **מחזיק לעניין מאגר מידע**- מי שמצוי ברשותו מאגר מידע דרך קבע, והוא רשאי לעשות בו שימוש. מדובר בספק ששומר את המידע או מעבד אותו עבור בעל המאגר ולפי הוראותיו. (סעיף 3 לחוק הגנת הפרטיות התשמ"א-1981)

4.6 **ספק חיצוני** - כל אדם/ חברה המועסקים על ידי רשות מקרקעי ישראל ומקבלים תשלום על ביצוע עבודות או אספקת שירותים / מוצרים. הספק יכול לפעול באחת מהצורות הבאות:

4.6.1 נותני שירותים - עובדים של חברה חיצונית המעניקים שירות חד פעמי, או מתמשך, אך אינם יושבים דרך קבע במשרדי רשות מקרקעי ישראל.

4.6.2 הענקת שירותי מחשוב ללא הגעה פיזית לאתר.

4.7 **היפטרות (Disposal) ממדיות**- גריטת מדיה מגנטית או מחיקת מידע באופן שאינו מאפשר את שחזורו ממדיה מגנטית, המכילה מידע חסוי/חסוי אישי ו/ או מידע פנימי ו/או מידע חסוי ביותר.

4.8 **תווך**- מרחב להעברת נתונים ממקום למקום לצורך תקשורת (באמצעות כבל או גלי רדיו).

5 אחריות

5.1 ממונה הגנת הסייבר יתווה תהליכים ושיטות טיפול הגנתי בממשקים עסקיים, לרבות:

5.1.1 קריטריונים להגדרת רגישות / סיווג הממשק העסקי.

5.1.2 דרישות הגנתיות בכפוף לסיווג הממשק העסקי.

5.1.3 שיטות וכלים לאכיפת הדרישות.

5.1.4 תהליכים ואמצעים לפיקוח, תיעוד ובקרה ולטיפול בחריגים.

5.2 באחריות המנהלים ברשות לעדכן את מנהל הגנת הסייבר אודות כוונה לבצע רכש של מוצרים או שירותים, לרבות שדרוג, תחזוקה או החלפת ספקים.

5.3 בחינת הצורך בשילוב היבטי הגנה כחלק מתהליך הרכש הינה באחריות מנהל הגנת הסייבר.

5.4 ניסוח פרק הגנת הסייבר בחוזה יתבצע ע"י ממונה הגנת הסייבר בסיוע המחלקה המשפטית וגורמי הרכש.

5.5 מנהל הגנת הסייבר יהיה אחראי על טיפול בהיבטי הגנת הסייבר בשרשרת האספקה.

5.6 הסמכות לאישור התקשרות חוזית חדשה מול ספק חיצוני הינה של ראש תחום טכנולוגיות.

5.7 הסמכות לאישור כל חריגה מהנחיות נוהל זה הינה של ממונה הגנת הסייבר או מי מטעמו.

6 <u>תחולה</u>

הנוהל חל על כל בעלי התפקידים ברשות מקרקעי ישראל.

ב. שיטה

7. <u>התקשרות עם ספק</u>

7.1. כל התקשרות עם ספק חיצוני, לצורך הספקת שירותים מסוג כלשהו, אשר במסגרתם תינתן גישה למתחמי ולמשרדי רשות מקרקעי ישראל, ו/או למערכות המידע ו/או לנכסי המידע של הארגון, תותנה בהתקשרות חוזית מקדימה, שתאושר ע"י האגף המשפטי של הרשות.

7.2. הספקים ברשות מקרקעי ישראל יסווגו בהתאם לרמת הרגישות של המידע אליו הם ניגשים:

7.2.1. ספק ברמת סיכון גבוהה- ספק הניגש אל מערכות המידע של הרשות ו/או מחזיק במידע של הרשות.

7.2.2. ספק ברמת סיכון נמוכה- ספק שאינו ניגש אל מערכות המידע של הרשות ואינו מחזיק במידע של הרשות.

7.3. הסכם ההתקשרות ייעשה בכתב ותינתן התייחסות לנושאים הבאים לכל הפחות:

7.3.1. הגדרת תחומי אחריות של כל אחד מהצדדים להסכם, לרבות קבלני המשנה.

7.3.2. הגדרת רמת שירות (Service Level Agreement), לרבות הגדרת שירותים, היקפם וזמני הספקתם על ידי הספק, ו/או על ידי קבלן המשנה ללקוח (הרשות) במצב חירום, הן של הרשות והן של הספק.

7.3.3. ספקים הנותנים שרות למערכות הרשות יחויבו בעמידה ברמת אבטחה של הארגון, טרם תחילת עבודתן על מערכותיו.

7.3.4. חובת הסודיות, הגנת סייבר ומצבי חירום.

7.3.5. דגש מיוחד יינתן בהתקשרות של הרשות עם ספקים, אשר מוגדרים ברמת סיכון גבוהה (ראה סעיף 2).

7.3.6. הסדרים להפסקת ההסכם וליישוב מחלוקות.

7.3.7. הסכמת ספק נותן השירותים, באם יתבקש לכך, לביצוע ביקורות במתחמיו ומשרדיו מטעם הרשות.

8. <u>שילוב פרק אבטחת מידע בהתקשרות עם ספק</u>

6.1 באחריות ממונה הגנת הסייבר בסיוע המחלקה המשפטית וגורמי הרכש, לכלול בחוזה ההתקשרות, פרק העוסק בנושא שמירת סודיות והגנת סייבר.

8.1. במידה ומדובר בהתקשרות לטובת ביצוע **רכש** עבור הארגון, גורמי הרכש הרלוונטיים יוודאו הוספת פרק, המסדיר את היבטי מתן השירות והסדרי אבטחת המידע טרם חתימה על החוזה. על פי הצורך, ייכתב פרק ייעודי בהתייעצות עם ממונה הגנת הסייבר ברשות מקרקעי ישראל.

8.2. במידה ומדובר בהתקשרות לטובת ביצוע **פעילות תמיכה או תחזוקה טכנית**, במסגרתה נדרשת גישה למערכות המחשוב, בחוזה ההתקשרות יתועדו לכל הפחות הפרטים הבאים:

8.2.1. פירוט של מהות ואופי ההתקשרות (שירותי תמיכה, תחזוקה ועוד).

8.2.2. פירוט המערכות עבורן יבוצע השירות.

8.2.3. הרשאות הגישה הנדרשות לביצוע הפעילות.

8.2.4. פרטי העובדים של הספק שיבצעו את הפעילות.

8.2.5. מסגרת פעילות התחזוקה השוטפת שתיכלל במסגרת השירות.

8.3. פרטים אלו יועברו לידיעת ממונה הגנת סייבר ברשות מקרקעי ישראל ובהתאם לכך ייכתב פרק / נספח ייעודי להגנת הסייבר.

8.4. במידה והסכם ההתקשרות עם הספק, כולל בתוכו **גישה למידע ו/או למערכות מידע** של הרשות, יש לבדוק את כל היבטי הגנת הסייבר, ולחתום על הסכם סודיות בין הרשות לבין הספק. ההסכם מעגן בתוכו, לפחות, התייחסות לסעיפים הבאים:

8.4.1. גישה למידע רגיש/ חסוי של הרשות.

8.4.2. חשיפה למידע רגיש/ חסוי של הרשות.

8.4.3. שמירת סודיות מידע רגיש/ חסוי של הרשות.

8.5. אם במהלך ההתקשרות הספק **ייחשף למידע רגיש ו/או חסוי,** הסכם ההתקשרות יביא בחשבון את האופי הרגיש. ההסכם יעגן בתוכו התייחסות לסעיפים הבאים:

8.5.1. שמירה על חיסיון המידע הרגיש ו/או חסוי ללא הגבלה בזמן.

8.5.2. הגבלות הגישה למידע רגיש ו/או חסוי.

8.5.3. כמו כן, בחוזה יוגדרו: בקרות אבטחה, רמת שירות ואספקה, חובת דיווח על אירועי הגנת סייבר הנוגעים לרשות.

8.6. במקרים בהם נאלצת הרשות למסור **נתונים הכלולים במאגרי המידע הרשומים** שלה:

8.6.1. הרשות תידרש לרשום את הספק כמחזיק לעניין מאגרי מידע בפנקס המאגרים. ראה נוהל א-18 תאימות ומאגרי מידע.

8.6.2. הספק ימציא תצהיר בדבר החזקת מאגר מידע.

8.6.3. צוות אבטחת מידע יגדיר את האיומים והסיכונים הנובעים מסוג המידע המועבר לספק ולקבוע אמצעי אבטחת המידע להתמודדות עימם. ככל שרמת רגישות המידע גבוהה יותר והנזק הצפוי להיגרם לנושא המידע עם חשיפתו יהיה גדול יותר, יש ליישם אמצעי אבטחת מידע יותר קפדניים.

8.6.4. בעל המידע יגדיר במפורש את המטרות המותרות לשימוש וסוג בעלי התפקידים המועסקים על ידי הספק שיהיו מורשים בגישה אל המידע של הרשות, וזאת על מנת להקפיד שהספק ישתמש במידע אך ורק לשם ביצוע המטרה המקורית של הפעילות שביצועה הועבר אליו.

8.6.5. באחריות המחלקה המשפטית לוודא כי חוזה ההתקשרות עם הספק מכיל בטוחות, לרבות חיוב עריכת ביטוח אחריות מקצועית, סעדים וכלי בקרה אפקטיביים שיאפשרו תגובה מהירה ויעילה של הרשות להפרות של הוראות החוק והחוזה.

8.6.6. במקרים הנדרשים, על הרשות לוודא כי לא קיים ניגוד אינטרסים כלשהו המונע את העברת המידע לספק.

8.6.7. במקרה בו הספק אוסף מידע ישירות מבעל המידע, על הרשות לוודא כי הספק יקיים ויקפיד הקפדה יתרה על קיום חובת ההודעה בפניה לאדם לקבלת מידע לשם החזקתו או שימוש בו במאגר מידע, הקבועה בסעיף 11 לחוק הגנת הפרטיות.

8.6.8. נוסח ההודעה ואופן קיומה צריכים להיקבע על ידי הרשות, או להיות מאושרים על ידה.

8.6.9. על ההודעה להכיל את הסעיפים הבאים:

8.6.9.1. אם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו.

8.6.9.2. המטרה אשר לשמה מבוקש המידע.

8.6.9.3. למי יימסר המידע ומטרות המסירה.

8.6.10. הרשות תקבע מראש הוראות ונהלים ביחס למימוש זכויות העיון והתיקון על ידי נושא המידע, כולל התייחסות לעניין זמני תגובה ועלויות.

8.6.11. במידה ונשוא המידע יפנה אל הרשות, עליה להפנות בכתב את מבקש המידע אל הספק שמוגדר כמחזיק, תוך ציון מענו, ולחייב את הספק לאפשר למבקש את העיון במידע.

8.7. לא תתאפשר גישה מרחוק עבור ספקים חיצוניים למערכות המידע של הרשות, ללא אישור מנהל הגנת הסייבר.

8.8. להלן טבלת עזר לניתוח משמעויות הגנת סייבר במכרזים:

קטגוריית התקשרות	נספח אבטחת מידע בחוזה
רכש עבור הארגון	סעיף- 2 דרישות כלליות
התקשרות במסגרתה מועבר מידע חסוי אישי הכלול במאגרי המידע הרשומים של הרשות.	סעיף- 2 דרישות כלליות סעיף 3- העברת מידע הרשום במאגרי המידע של הרשות
מערכת שעתידה להתארח בממשל זמין	סעיף1- דרישות ממשל זמין
מערכות Web ו WS	סעיף 4- דגשים למערכות Web ו WS
מערכת "ניהול הצעות מקוונות"	סעיף 5- הנחיות פרטניות למערכת "ניהול הצעות מקוונות"
מוצרים ותוכנות	סעיף 6- דרישות אבטחת המידע ממוצרי ותוכנות
התקשרות במסגרתה מועבר מידע חסוי ו/או חסוי ביותר ו/או פנימי.	סעיף- 2 דרישות כלליות
פעילות תמיכה או תחזוקה טכנית, במסגרתה נדרשת גישה למערכות המחשוב מרחוק.	סעיף- 2 דרישות כלליות
פעילות תמיכה או תחזוקה טכנית, המתבצעת ממתחמי הרשות.	סעיף- 2 דרישות כלליות

שהייה במתחמי הרשות וגישה למידע ו/או למערכות מידע של הרשות.	סעיף- 2 דרישות כלליות
שהייה במתחמי הרשות וחשיפה למידע חסוי ו/או פנימי.	סעיף- 2 דרישות כלליות
הקמת מערכת בענן	סעיף 2- דרישות כלליות, כולל סעיף 2.4.5- אבטחה פיזית סעיף 7- הקמת מערכת בענן

9. <u>התחייבות לשמירה על סודיות המידע במסגרת התקשרות עם ספקים חיצוניים</u>

9.1.1. נציגי הספק יוחתמו על הצהרה לשמירת סודיות המידע בשם הספק (ראה נספח ב').

9.1.2. על פי מכרז חשכ"ל, נציגי הספק יוחתמו על הצהרה לשמירת סודיות המידע בשם החברה (ראה נספח ג').

9.1.3. בעת התקשרות למתן שירותים במערכות מידע רגישות ו/או חשיפת עובדי הספק למידע ארגוני בעל רגישות גבוהה, יתחייב הספק למסור את שמות העובדים שיועסקו בפעילות ובמידת הצורך, עובדים כל אחד מעובדים אלה יוחתמו על הצהרה, בה הם מתחייבים לשמירה על סודיות (ראה נספח א').

10. <u>ליווי פעילות עובדים במסגרת התקשרות עם ספקים חיצוניים</u>

10.1. יועצים

10.1.1. תהליך הקליטה של עובדי מיקור חוץ, יהיה דומה לתהליך קליטת עובדי הרשות, זאת בנוסף לבדיקות ולחוזה שייחתם עם חברתם.

10.1.2. יועצים יבצעו מבדקי מהימנות, בהתאם לצורך ולדרישת הרשות.

10.2. עובדים מזדמנים

10.2.1. אין לאפשר לספק השירות גישה למערכות ולציוד, אשר לא הוגדרו מולו במפורש בחוזה השירות.

10.2.2. הספק יגדיר צוות עובדים אשר חבריו יחתמו על הסכם סודיות עם רשות מקרקעי ישראל. עובדים אלה בלבד יורשו לספק שירותים עבור רשות מקרקעי ישראל. באחריות מזמין השירות ברשות לוודא ביצוע הוראה זו.

10.2.3. בעת מתן השירות למערכות המחשוב של הרשות, ע"י ספק חיצוני, ילווה עובד הספק ע"י נציג צוות טכנולוגיות או צוות הפעלה או גורם אחר מטעם הרשות, אשר מכיר היטב את תחום העיסוק בו נערכת הפעילות, ויכול לבצע בקרה אפקטיבית אחר פעילותו של עובד הספק.

11. <u>הקמת חשבון משתמש במסגרת התקשרות עם ספקים חיצוניים</u>

11.1. לכל ספק חיצוני, בהתאם לצורך ולאופי השירות, ייפתח חשבון משתמש ייעודי, יונפקו אמצעי זיהוי נדרשים (כרטיס חכם לנותן שירותים, טוקן או כל אמצעי מקובל אחר) ויוגדרו הרשאות מתאימות, המאפשרות ביצוע פעולות ו/או גישה למידע, הנדרשים לצורך ביצוע התפקיד בלבד. לפירוט ראה נוהל א-9 בקרת גישה.

11.2. על עובד הספק חל איסור לבצע שימוש בחשבון של בעל תפקיד ברשות מקרקעי ישראל לצורך ביצוע פעילות כלשהי.

11.3. באחריות בעל התפקיד מטעם הרשות, המלווה את הפעילות, לוודא כי לא נעשה שימוש לרעה בחשבון המשתמש של הספק ולפקח באופן רציף על פעילות הספק החיצוני, באמצעות ביצוע בקרת פעילות במסגרת בקרת הרשאות.

11.4. במידה ונדרשת גישה של הספק למערכת באופן סדיר, יינתן חשבון משתמש אישי לכל אחד מעובדי הספק.

11.5. באחריות מנהל דלפק סיוע, בהנחיית ראש תחום טכנולוגיות או מי מטעמו, להגדיר את "שם המשתמש" לעובדי הספק.

12. <u>מתן הרשאות גישה במסגרת התקשרות עם ספקים חיצוניים</u>

12.1. הרשאות הגישה לספקים החיצוניים יוגדרו ע"י דלפק הסיוע, בהנחיית ראש תחום טכנולוגיות או מי מטעמו, ויאפשרו ביצוע פעילות מוגדרת בלבד, תוך מתן גישה למערכות ולמידע ההכרחיים, בלבד, לצורך ביצוע הפעילות.

12.2. חשבון המשתמש, וההרשאות הנגזרות ממנו, תהיינה לתקופה מוגבלת, על פי המוגדר בהסכם ההתקשרות.

12.3. הרשאות הגישה של עובדי הספקים החיצוניים, אשר אינם עובדים באופן קבוע ברשות, יהיו במצב מושהה (In Active) כברירת מחדל. ההרשאות ישוחררו לפרק זמן קצוב, בו תבוצע הפעילות על ידי עובדי הספק, כאשר לאחר גמר הפעילות ההרשאות יוקפאו שוב.

13. <u>גישה מרחוק למערכות המחשוב במסגרת התקשרות עם ספקים חיצוניים</u>

13.1. ככלל, כל חיבור חיצוני למערכות המחשוב וציוד התקשורת של רשות מקרקעי ישראל ייעשה באישור גורם הגנת הסייבר ברשות מקרקעי ישראל.

13.2. תצורת התחברות, או גישה מרחוק, תאושר ותאופיין ע"י גורם הגנת הסייבר, זאת על מנת למנוע סיכוני אבטחה בתהליך הגישה מרחוק.

13.3. נציג תחום הגנת הסייבר יגדיר את השימוש בכלל האמצעים והטכנולוגיות הנדרשות על מנת לאפשר חיבור מאובטח לרשת המחשוב של הארגון.

13.4. בכל התחברות מרחוק של ספק חיצוני למערכות מידע ו/או ציוד תקשורת של הרשות, יבוצע מעקב ותיעוד בעזרת כלי ניטור ממוכן, בהתאם לסטנדרטים הנהוגים בשוק ובהתאם להחלטת מנהל הגנת הסייבר. אלה

יבוצעו אחר כל הפעולות שבוצעו על ידי הספק החיצוני במערכת לאורך כל זמן החיבור מרחוק לרשת המחשבים של הארגון (ראה פירוט מטה בסעיף 'בקרה').

13.5. במערכות שבהן מופעל רישום לוגים, יש לבצע מעקב שוטף, ורישום הפעולות הרגישות והחריגות המתבצעות במערכת על ידי גורמים חיצוניים. (לדוגמא: התחברות שלא בשעות העבודה והאם הייתה פנייה מתועדת מהרשות, זיהוי פעולות שהתבצעו תוך שימוש בשם המשתמש של הספק וכו').

13.6. עבור כל סוג התחברות מרחוק, באחריות צוות טכנולוגיות או צוות הפעלה או דלפק סיוע (בהתאם לתחום הפעילות) לתעד את הפרטים הבאים:

13.6.1. פירוט מהות ואופי ההתחברות מרחוק.

13.6.2. תיאור תצורת ההתחברות מרחוק של הספק למערכות הרשות.

13.6.3. פירוט המערכות עבורן בוצע השירות.

13.6.4. הרשאות הגישה המדויקות הנדרשות לביצוע הפעילות.

13.6.5. פרטי העובדים של הספק שיבצעו את הפעילות ואופן זיהויים בעת ההתקשרות.

13.6.6. פעילות התחזוקה השוטפת שתיכלל בשירות, לרבות זמני עבודה.

13.6.7. אופן התיעוד של כל גישה מרחוק של הספק.

14. <u>אבטחת תווך התקשורת במסגרת התקשרות עם ספקים חיצוניים</u>

14.1. בכל התחברות מרחוק למערכות המחשוב של רשות מקרקעי ישראל, תווך התקשורת יוצפן, לרבות הצפנת סיסמאות מורשי הגישה.

14.2. אמצעי ההצפנה ו/או רמת ההצפנה הנדרשת יוגדרו ע"י גורם הגנת סייבר ברשות, בהנחיית יה"ב או בהתאם לסטנדרטים המקובלים בשוק.

15. <u>פעילות בקרה במסגרת התקשרות עם ספקים חיצוניים</u>

15.1. על הרשות לוודא, כי הספק החיצוני שומר על עקרונות אבטחת מידע נאותים בכלל, ועומד בהנחיות אבטחת המידע, כפי שהוגדרו לו על ידי הארגון בפרט, זאת על מנת להגן על נכסי המידע של הרשות ושל לקוחותיה מפני דליפה, שינוי או מחיקה.

15.2. על מנת לוודא כי מחויבות זו נשמרת, באחריות צוות אבטחת מידע או מי מטעמם לבצע ביקורות מתוכננות וביקורות פתע על פעילות הספק.

15.3. כאשר מדובר בספק שעובדיו ניגשים מרחוק לרשת הרשות, ו/או בספק המחזיק אצלו מידע רגיש ו/או מסווג של הרשות, יתבצע מבדק אבטחת מידע לאיתור הסיכונים שיכולים לנבוע מהתהליך.

15.4. יש לבצע מבדקי אבטחת מידע גם אצל ספקים המוסמכים לתקן ISO 27001 לניהול מערכת אבטחת מידע.

15.5. כאשר מדובר בהתקשרויות עם ספקים שזכו במכרז חשכ"ל, הביקורת אצל הספק מבוצעת במסגרת המכרז, ובהתאם לדרישות המכרז.

15.6. לפני קישור הספק למערכות הרשות, תבוצע ביקורת באתר ממנו מתחבר הספק על ידי מנהל הגנת הסייבר או בא כוחו. על בסיס ממצאי הביקורת, מנהל הגנת הסייבר יגדיר את אמצעי אבטחת המידע הנדרשים.

15.7. הבדיקות יתמקדו בנושאים הבאים (ראה נספח א'- שאלון לבדיקת הגנת סייבר בחצרות הספק):

15.7.1. ניהול אב"מ, מדיניות ונהלים.

15.7.2. אבטחת משאב האנושי.

15.7.3. אבטחה פיזית.

15.7.4. שינוע והעברת המידע מ/אל הספק.

15.7.5. אבטחת תפעול ותקשורת.

15.7.6. ניהול גיבויים.

15.7.7. אבטחת רשתות סלולאריות.

15.7.8. בקרת גישה.

15.7.9. אבטחת גישה מרחוק.

15.7.10. ניטור ומעקב.

15.7.11. היפטרות (Disposal) ממדיות ומניירת והוצאת מידע מחצרות הספק.

15.8. יש לוודא באמצעות ביקורת ספק תקופתיות, כי רמת הגנת הסייבר של הארגונים החיצוניים המתממשקים לרשת הפנימית, או שומרים על גבי הרשת הפנימית שלהם מידע של רשות מקרקעי ישראל יעמדו בנהלי הרשות למקרקעי ישראל.

15.9. יש ליצור, במידת האפשר ובהתאם לסיווג המידע, סביבת עבודה ייעודית אצל החברה החיצונית המתחזקת ו/או תומכת במערכות רמ"י, אשר תהיה מנותקת מרשת החברה המתחזקת. סביבה זו תהיה היחידה אשר ממנה ניתן יהיה להתחבר לרשת של רשות מקרקעי ישראל.

15.10. ביקורות תקופתיות יבוצעו אצל החברה החיצונית, בהתאם להחלטת מנהל הגנת הסייבר, על ידי הרשות או מי מטעמו ובהתאם לפרמטרים שהוסכם עליהם בחוזה העבודה מול הספק (ראה סעיף 2.8).

15.11. בהתאם לאופי ורגישות ההתקשרות יופעל תהליך בקרה, ניטור ותיעוד (Audit) על חשבון המשתמש של עובדי הספק החיצוני, על פי הגדרות גורם הגנת סייבר ו/או ראש תחום טכנולוגיות ברשות.

15.12. גורם הגנת סייבר ברשות יוודא כי חשבונות המשתמש של עובדי הספק החיצוני ברשות ובחצרות הספק עומדים בכלל דרישות האבטחה, אשר הוגדרו עבור חשבונות של בעלי התפקידים ברשות, לרבות קבועי זמן להחלפת סיסמא, מורכבות הסיסמא ועוד, באמצעות ביצוע ביקורות ספק תקופתיות וביצוע סקרי הרשאות.

15.13. אחת לשנה, יבחן גורם הגנת סייבר ברשות את תוקפם של הסכמי ההתקשרות עם ספקים חיצוניים ותוקפם של "שמות המשתמשים" שלהם במערכות המחשוב.

15.14. אם ימצא עובד ספק חיצוני, המועסק שלא במסגרת הסכם התקשרות, תושעה מידית גישתו למערכות המידע של הרשות. מתן גישה מחודשת תתאפשר רק לאחר ביצוע ההתקשרות מחודשת כנדרש.

16. <u>הערכה וטיפול בחשיפות אבטחה</u>

16.1. ממצאים/ חשיפות אבטחה יוערכו לשלוש רמות (גבוה, בינוני, נמוך) בהתחשב בהסתברות לסיכון ובעוצמת הסיכון, כמפורט במתודולוגיה לניהול סיכוני אבטחת מידע וכן יתועדו במערכת הרשות.

17. <u>סיום התקשרות עם ספקים</u>

17.1. מידע וציוד השייכים לרשות מקרקעי ישראל יוחזרו לגורמים הרלוונטיים בסיום תקופת עבודתו של הספק/ היועץ.

17.2. חריגה מהאמור לעיל תהווה הפרה של ההסכם שנחתם בין הספק לרשות מקרקעי ישראל.

17.3. באחריות מנהל היחידה המקבלת את השירות להודיע למנהל הגנת הסייבר על סיום הפרויקט ו/או סיום

17.4. ההתקשרות עם הספק.

17.5. מנהל הגנה בסייבר יוודא כי הספק נותק מרשת הרשות למקרקעי ישראל.

נספחים

18. נספח א'- שאלון לבדיקת הגנת סייבר בחצרות הספק

נושא	תת נושא
כללי	האם יש ניהול לתחום אב"מ
	האם הארגון מוסמך ISO 27001
	האם מבוצעים מבדקי חדירה לארגון
	אם כן - ע"י מי
	למי מועברות התוצאות וההמלצות
סיסטם	מי קובע נהלי עבודה ברשת - AV, FW, עדכוני גרסה וכד'
	מי אוכף עבודה ע"פ הנהלים הללו
	האם יש חיבור לרשתות נוספות
	האם יש גיבויים למידע
	מי אחראי לגיבויים
	זמן מהגיבוי האחרון RPO - Recovery Point Objective
	זמן התאוששות לאחר נפילה RTO - Recovery Time Objective
	האם יש כספות מידע
	מי מורשה גישה לכספות
	מי מנהל את רשימת מורשי הגישה לכספות
	האם יש גישה מרוחקת למאגרי המידע
	מי מגדיר את נהלי הגישה
	מי מפקח על עבודה ע"פ הנהלים הללו
	האם קיים מנגנון ניטור ומעקב
	האם יש רשתות אלחוטיות
	האם הכניסה אליהם מוגנת סיסמה
	האם יש נוהל עדכוני גרסאות, האם הוא נאכף
הגנת מידע	איך נכנסים למחשב
	אורך הסיסמה
	האם יש מחשבים פתוחים ללא השגחה
	סיכוי פעולה זדונית בעקבות כך
	האם יש מסמכים רגישים ללא השגחה
	האם יש העברת כרטיסים בין העובדים
	האם יש נוהל חסימת כרטיס לעובד שעוזב
	האם יש גישה לעובדים לא מורשים לחומר מסווג
ספקי משנה	האם קיימת עבודה מול ספקי משנה
	האם יש נהלי עבודה מול ספקים אלו
	האם נדרש שינוע חומר בצורה ידנית
	האם יש תהליך מוגדר לשינוע חומרים אלו

19. נספח ב'- התחייבות לשמירה על סודיות

טופס הצהרת סודיות

אני הח"מ _____, הנושא תעודת זהות מספר _____, המועסק בתאגיד _____, בתפקיד _____, מצהיר בזאת:

1. הואיל והתאגיד בא בקשר עסקי עם רשות מקרקעי ישראל (להלן - "הרשות") לאספקה של שירותים ו/לקבלת מידע בדבר מערכות הרשות (להלן – "השירותים") והואיל וידיעות ומידע, שהגיעו או יגיעו אלי עקב העסקתי בתאגיד, או שיווצרו בתאגיד עקב ביצוע האמור, הינם בגדר מידע רגיש / חסוי והינם בגדר סוד.
2. לפיכך, אני הח"מ מצהיר בזאת, שכל ידיעה, אשר בידי או תגיע לידי תוך כדי הכנת ההצעה לאספקה של השירותים לרשות או עקב מתן השירותים בפועל היא בסיווג מידע רגיש / חסוי ואני מתחייב לשמור עליהן בסוד. התחיבותי זו חלה הן לגבי נתונים והן לגבי כל סוגי המידע האחרים אשר יגיעו לידיעתי בתוקף עבודתי כאמור.
3. תשומת לבי הופנתה לחוק העונשין (התשל"ז - 1977) (להלן - "החוק") ובמיוחד - לסעיפים 118 ו-119, המובאים להלן:

סעיף 118: **גילוי בהפרת חוזה:**

א. היה אדם בעל חוזה עם המדינה או עם גוף מבוקר כמשמעותו בחוק מבקר המדינה התשי"ח - 1958 (נוסח משולב) ובחוזה יש התחיבות לשמור בסוד ידיעות שיגיעו אליו עקב ביצוע החוזה, והוא מסר ללא סמכות כדין ידיעה כאמור לאדם שלא היה מוסמך לקבלה, דינו - מאסר שנה אחת.

ב. בסעיף זה "בעל חוזה" לרבות מי שהועסק כעובד או כקבלן לשם ביצוע החוזה, ואולם תהא זו הגנה טובה לנאשם לפי סעיף זה שלא ידע על ההתחיבות לשמור ידיעות כאמור בסוד ושהוא מסר את הידיעה בתום לב.

סעיף 119: **גילוי בהפרת אימון:**

מי שנמסר לו מסמך רשמי בתנאי מפורש שעליו לשומרו בסוד והוא מסרו לאדם שאינו מוסמך לקבלו, דינו - מאסר שנה אחת. התרשל בשמירתו או שעשה מעשה שיש בו כדי לסכן בטיחותו של המסמך, דינו - מאסר ששה חודשים.

"ידיעה" - לרבות ידיעה שאינה נכונה וכל תיאור, תכנית, סיסמה, סמל, נוסחה, חפץ או חלק מהם המכילים ידיעה או העשויים לשמש מקור לידיעה.

"מסירה" - לרבות מסירה ע"י סימון ואיתות ומסירה עקיפה.

4. אני מתחייב לשמור בסוד, לא להעביר, לא להודיע, לא למסור ולא לגלות ולא לגרום לגלוי למאן דהו, בישראל ומחוצה לה, כל ידיעה כנ"ל וכל מידע, אשר יגיעו לידיעתי, תוך משך תוקפה של הצהרה זו וכן לאחר תום תוקפה ובכל עת, אלא אם כן נתקבל אישור מראש ובכתב על גלוי ידיעה כנ"ל מאת נציג הרשות.
"גלוי" - לרבות מסירת מידע על נתונים, תכניות ישומיות ומערכות המחשוב של הרשות ואמצעי האבטחה שלהן, פרסום ברבים לקידום מכירות, הצגת מסמכים וחוזים לצורך קבלת אשראי מבנקים, מסירת ידיעות לכלי התקשרות, פרסום מאמרים בעתונות כללית ומקצועית, כתבות משודרות והרצאות.

5. ידוע לי, כי מותר יהיה לגלות כל ידיעה כאמור רק למי שהתחייב לשמור עליה בסוד, הכל בכפוף להצהרה זו ולצרכי עבודה בלבד ולאחר קבלת הסכמתו המפורשת בכתב ומראש של הרשות. בכל מקרה אחר, אני מתחייב שלא לגלות את הידיעה, אלא אם קיבלתי לכך אישור מפורש ובכתב מנציג הרשות.

6. אני מתחייב לפעול בהתאם להוראות החוק להגנת הפרטיות והוראות כל חוק, הנוגע לענין.

ולראיה באתי על החתום, לאחר שקראתי בעיון את הכתוב בהצהרה זו והתחייבתי לנהוג על פיה.

_____	_____	_____
תאריך	**שם החותם**	**חתימה**

אישור עו"ד

אני הח"מ_____, עו"ד, מספר רישיון _____ מאשר בזאת כי ביום _____ הופיע בפני מר/גב'_____ אשר זיהה עצמו באמצעות ת.ז. שמספרו _____/ המוכר לי אישית, ולאחר שהזהרתיו לומר את האמת וכי יהיה צפוי לעונשים הקבועים בחוק אם לא יעשה כן, אישר בפני את נכונות הצהרתו וחתם עליה.

תאריך	שם מלא של עו"ד	חתימה וחותמת

20. נספח ג' – התחייבות לשמירה על סודיות חשכ"ל

הצהרה לשמירה על סודיות

שנערכה ונחתמה ב_____ ביום ____ בחודש _____ שנת_____

על ידי _____

ת.ז. _____

מכתובת _____

הואיל וממשלת ישראל בשם מדינת ישראל מקבלת את השירותים/הטובין כהגדרתם להלן;

והואיל והנני מועסק בקשר למתן השירותים/הספקת הטובין;

והואיל והנני עשוי להיחשף לסודות מקצועיים עליהם מעוניינת מדינת ישראל להגן;

לפיכך הנני מתחייב כלפי מדינת ישראל כדלקמן:

1. הגדרות

בהתחייבות זו תהיה למונחים הבאים המשמעות המופיעה לצידם:

"השירותים/הטובין" - ההגדרה תושלם לכל מכרז בהתאם לצורך.

_____

_____

_____

"עובד" - כל אחד מעובדי הקבלן אשר באמצעותו יינתנו השירותים למזמין.

"מידע" - כל מידע (Information), ידע (Know-How), ידיעה, מסמך, תכתובת, תוכנית, נתון, מודל, חוות דעת, מסקנה וכל דבר אחר כיוצ"ב הקשור או הנוגע למתן השירותים/הספקת הטובין בין בכתב ובין בע"פ בכל צורה או דרך של שימור ידיעות בצורה חשמלית, אלקטרונית, אופטית, מגנטית או אחרת.

"סודות מקצועיים" - כל מידע אשר יגיע לידי הקבלן או העובד בקשר למתן השירותים/הספקת הטובין, בין אם נתקבל במהלך מתן השירותים/הספקת הטובין או לאחר מכן, לרבות ומבלי לפגוע בכלליות האמור לעיל: מידע אשר ימסר ע"י המזמין, כל גורם אחר או מי מטעמו.

2. שמירת סודיות

הנני מתחייב לשמור את המידע או הסודות המקצועיים בסודיות מוחלטת ולעשות בהם שימוש אך ורק לצורך מתן השירותים/אספקת הטובין נושאי מכרז זה. למען הסר ספק, ומבלי לפגוע בכלליות האמור, הנני מתחייב לא לפרסם, להעביר, להודיע, למסור או להביא לידיעת כל אדם את המידע או הסודות המקצועיים.

הנני מצהיר כי ידוע לי שאי מילוי התחייבויותיי מהוות עבירה לפי פרק ז' (ביטחון המדינה, יחסי חוץ וסודות רשמיים) לחוק העונשין, תשל"ז - 1977.

הריני מצהיר כי ידוע לי, כי חשיפת מידע אישי המגיע לידי, לגורם שאינו מורשה לקבלו, עלולה להוות פגיעה בפרטיותו של אדם, עבירה שבגינה אני עלול להיתבע לדין על-פי סעיף 5 לחוק הגנת הפרטיות התשמ"א-1981.

ולראיה באתי על החתום: _____