נוהל: אבטחת מידע במיקור חוץ

גרסה:	1.0
כותב הנוהל:	תחום אבטחת מידע משרד התחבורה והבטיחות בדרכים
נבדק ע"י:	מנהל תחום אבטחת מידע, בלוג אריה
מאשר הנוהל:	מנהל חטיבת אבטחת מידע וסייבר, אלון ליכטנשטיין
תאריך הוצאה:	מרץ 2019
תאריך שינוי אחרון:	23.3.2019
מועד הסקירה הבאה:	מרץ 2020

ניהול גרסאות

תאריך	גרסה	מהות השינוי
23.3.2019	1.0	

1. כללי

1.1. כחלק מפעילותו, נעזר המשרד בספקי מיקור חוץ וגורמי צד ג' (להלן: "גורמים חיצוניים"). במסגרת זאת, הגורמים החיצוניים מספקים שירותים שונים ונחשפים למידע בעל רגישות משתנה של המשרד. כפועל יוצא, נדרש לנהל את הסיכונים השונים בתהליך זה, לרבות בהיבטי אבטחת מידע.

1.2. ויודגש, בעת השימוש בשירותי מיקור חוץ החובות והאחריות המוטלים מכוח חוק הגנת הפרטיות ותקנותיו על בעל מאגר מידע, מנהל מאגר מידע והמחזיק בו ממשיכים לחול על כל אחד מהם כאילו הוא מבצע את הפעילות בעצמו, כולל, בין היתר, חובת אבטחת המידע והבטחת מימוש זכויות נושא המידע.

2. סעיפים ישימים

2.1. ISO 27001- סעיף A.15.

2.2. תקנות הגנת הפרטיות- תקנה 15.

2.3. תורת ההגנה של מערך הסייבר- בקרות 16.1, 17.5.

3. מטרה

3.1. להסדיר את תהליך ההתקשרות של המשרד עם קבלנים , ספקים וגורמי צד ג' בהיבטי אבטחת מידע והגנה על הפרטיות.

4. תחולה

4.1. כלל עובדי ומנהלי הקבלן/ספק העושים שימוש במערכות מידע השייך למשרד.

4.2. קבלנים וגורמים חיצוניים מתוקף תקנה 15 (2) בתקנות הגנת הפרטיות התשע"ז (2017).

5. הגדרות ומושגים[1]

5.1. **אירוע אבטחה / סייבר**[2] – אירוע או חשד שנעשה בו שימוש במידע\ מערכת, בלא הרשאה או בחריגה בהרשאה או שנעשתה פגיעה בשלמות , זמינות או דלף מידע.

5.2. **בעל הרשאה** – יחיד או רבים אשר יש להם גישה למידע מהמאגר או מערכות המאגר על פי הרשאתו של בעל המאגר.

5.3. **מאגר מידע** – אוסף נתוני מידע, לרבות מספרי ת"ז ופרטי קשר, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב או אחר.

5.4. **מזמין** – כל עובדי המשרד ונציגיו, המבקשים להוציא פעילות תחזוקה\עיבוד של מידע או מערכות למיקור חוץ.

5.5. **מחזיק מאגר מידע** – מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש.

5.6. **מידע רגיש** – נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.

5.7. **נושא מידע** – מי שמוחזק עליו מידע במאגר המידע.

5.8. **סיכון סייבר** – סיכון לשימוש לא מורשה בזהות, הפרעה לפעילות הארגון על ידי פגיעה בפעילות הרשת ו/או במערכות מידע, גניבה של מאגרי מידע, החדרה של קוד זדוני ,חדירה למערכת מידע או חשיפת מידע

5.9. **קבלן/ספק** – אדם ו/או תאגיד, הנותן שירותי מיקור חוץ לעיבוד מידע , תחזוקת מערכות למשרד.

---

[1] מדינת ישראל – משרד המשפטים, "**חוק הגנת הפרטיות**", התשמ"א (1981).

[2] מדינת ישראל - משרד המשפטים, **"תקנות הגנת הפרטיות (אבטחת מידע)"**, התשע"ז (2017).

6. שיטה

<u>דרישות אבטחה מגורמים חיצוניים</u>

6.1. באחריות אבטחת מידע משרד התחבורה להגדיר את רמת החשיפה של קבלנים וספקים למידע של המשרד, לרבות:

6.1.1. רמת הסיווג אליה יכול להיחשף הקבלן/ספק.

6.1.2. אופן גישת הקבלן/ספק למידע של המשרד ומערכותיו, למשל: גישה פיזית ללא ליווי, גישה מרחוק תוך שימוש בהתחברות מאובטחת ועוד.

6.1.3. אופן ניטור גישת הגורם החיצוני למידע ולמערכות מידע של המשרד.

6.2. באחריות משרד התחבורה למפות ולזהות את האיומים והסיכונים הנובעים משימוש במערכת/שרות הקבלן/ספק על האספקטים הטכנולוגיים והתהליכים הגלומים בהם כחלק מתהליך ניהול הסיכונים הארגוני, תתבצע הבחנה בין סוגי הקבלנים/ספקים השונים כגון : מעבד/מחזיק מידע, ספק תמיכה/פיתוח, ספק שירותים בענן.

6.3. באחריות אבטחת מידע משרד התחבורה להגדיר את דרישות האבטחה המינימליות מהגורם החיצוני, בשיתוף הגורמים הבאים:

6.3.1. קב"ט - בכל הקשור לסינון בטחוני, אבטחה פיזית וכו'.

6.3.2. מחלקת תפעול ותשתיות - בכל הקשור לגישה מרחוק, חשבון משתמש וכו'.

6.4. הקבלן מסכים להגדרות תהליך לניטור ובקרת רמת עמידת הקבלן בדרישות האבטחה. במסגרת תהליך זה, ניתן להשתמש באמצעים הבאים:

6.4.1. ביקורת חצרות קבלן \ ספק.

6.4.2. שאלונים לקבלן\ספק.

6.4.3. כלי ניטור ממוחשבים.

6.5. הקבלן\ספק מתחייב לעמוד בתקן ISO 27001 בהתאם להחלטת ממשלה 2443 , תקנות הגנת הפרטיות- תקנה, תורת ההגנה של מערך הסייבר- בקרות 16.1, 17.5.

6.6. הקבלן/ספק יעסיק גורם מקצועי בהיבטי אבטחת מידע שישמש איש קשר למשרד התחבורה בנושא זה.

6.7. הקבלן/ספק מתחייב לעמוד בדרישות החוק בדגש על חוק הגנת הפרטיות והתקנות הנגזרות ממנו , התחייבות זו תוגש ע"י תצהיר חתום של ממונה אבטחת המידע של הקבלן/ספק ומנהל החברה.

6.8. הקבלן/ספק מתחייב להגיש למשרד כל שנה דו"ח ביקורת חיצוני חתום ע"י גורם מוסמך ומקצועי (כל גורם המלווה ארגונים להסכמות אבטחת מידע) , מבנה הדו"ח מצורף **בנספח א'**.

6.9. החיבור של הקבלן/ספק לתשתית המידע של משרד יכלול את התכונות הבאות:

1) הזדהות חזקה (MFA) .

2) תקשורת מוצפנת .

3) באחריות הקבלן/ספק לוודא כי כל תקשורת בינו לבין המשרד עוברת תהליך סינון מתוכנות מזיקות.

4) באחריות הקבלן/ספק לנטר ולבקר את המשתמשים במערכות המידע, ידווח על אירועים חריגים למשרד התחבורה, והקמת יכולת להעברת לוגים של אירועי אבטחת מידע ל SOC הממשלתי ע"פ הגדרה של יה"ב.

5) הספק יסכים לביצוע הקלטה של תהליכי עבודה המתקיימות במערכות המידע של משרד התחבורה.

6) הספק מתחייב לעמוד בדרישות הגנת סייבר ספציפיות שיקבעו לפני תחילת העבודה מול חטיבת הגנת הסייבר במשרד.

<u>התייחסות להיבטי אבטחת מידע בעת חתימת הסכם שהקבלן/ספק צריך לקחת בחשבון</u>

6.10.בעת מענה למכרז\ הסכם על הקבלן לכלול בו התייחסות לנושאים הבאים:

6.10.1. פירוט המידע אשר יימסר לקבלן/ספק או שיהיה בעל גישה אליו.

6.10.2. סיווג המידע אשר יימסר לקבלן/ספק או שיהיה בעל גישה אליו.

6.10.3. כלל מחויבויותיו החוקיות והרגולטוריות של הקבלן/ספק, בהיבטי אבטחת מידע, שמירה על קניין רוחני, כמו גם פירוט באשר לאופן בו יבטיח הגורם החיצוני כי הוא עומד בהן.

6.10.4. מחויבות הקבלן/ספק בהסכם לאכוף שורה מוסכמת של בקרות, לרבות בקרת גישה, ניטור, מדידת ביצועים, דיווח וביקורת.

6.10.5. כללים לשימוש נאות במידע של המשרד, כמו גם הגבלות בנושא, למשל, איסור על שימוש במידע שלא למטרה לשמה נמסר לגורם החיצוני.

6.10.6. רשימה מפורטת של עובדי הקבלן/ספק בעלי הרשאות למידע של המשרד, או נהלים למתן אישור הרשאות גישה כמו גם הסרת הרשאות הגישה למידע.

6.10.7. נהלי אבטחת המידע של הקבלן/ספק המחייבים את עובדי החברה.

6.10.8. דרישות בהיבטי אירוע אבטחת מידע, בדגש על מתן הודעה למשרד ושיתוף פעולה בעת הטיפול באירוע.

6.10.9. על הקבלן/ספק לדווח על אירוע אבטחת מידע למשרד התחבורה באופן מידי בעת שעולה חשש לכך.

6.10.10.פעילות בהיבטי מודעות אבטחת מידע לעובדי החברה.

6.10.11.רשימת נוהלי אבטחת מידע רלוונטיים לעבודת הקבלן.

6.11.בהתאם לדרישות תקנה 15 (א) בתקנות הגנת הפרטיות התשע"ז (2017) – מיקור חוץ, בעל מאגר המתקשר עם קבלן לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע:

6.11.1. יבחן, לפני ביצוע ההתקשרות עם הקבלן המסוים כאמור, את סיכוני אבטחת המידע הכרוכים בהתקשרות – תקנה 15(א-1).

6.11.2. יקבע במפורש בהסכם עם הקבלן (בתקנה זו - ההסכם) את כל אלה, בשים לב לסיכונים לפי פסקה (1) – תקנה 15(א-2):

6.11.2.1. (א) הקבלן/ספק מבין ומכיר את המידע \ מערכות שהוא רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות.

6.11.2.2. (ב) הקבלן/ספק מכיר את מערכות המאגר שהוא רשאי לגשת אליהן.

6.11.2.3. (ג) הקבלן/ספק מבין את סוג העיבוד או הפעולה שהוא רשאי לעשות.

6.11.2.4. (ד) הקבלן/ספק מבין את משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו ודיווח על כך לבעל מאגר המידע.

6.11.2.5. (ה) הקבלן/ספק יציג את אופן יישום החובות בתחום אבטחת המידע להן הוא מחויב לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע המשרד והחוק.

6.11.2.6. (ו) חובתו של הקבלן/ספק להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם כאמור .

6.11.2.7. (ז) התיר המשרד לקבלן/ספק לתת את השירות באמצעות גורם נוסף - חובתו של הקבלן לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנות אלה.

6.11.2.8. על הקבלן/ספק לקבל את אישור משרד התחבורה את הגורם הנוסף עמו הוא מעוניין להתקשר.

6.11.2.9. (ח) חובתו של הקבלן לדווח, אחת לשנה לפחות, למשרד על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע למשרד במקרה של אירוע אבטחה.

6.11.3. הקבלן ינקוט אמצעי בקרה ופיקוח על עמידתו בהוראות ההסכם ובהוראות תקנות אלה, בהיקף הנדרש בשים לב לסיכונים ודרישות החוק.

ניהול שינויים לשירותים המסופקים על ידי הקבלן

6.12.שינויים להסכמים עם קבלנים, לרבות שיפור רמת האבטחה, צריכים להיות מנוהלים, להתחשב בקריטיות המידע, התהליכים והמערכות להם הם נוגעים, ולהעריך מחדש את סיכוני אבטחת המידע.

במסגרת זאת, יש לקחת בחשבון את ההיבטים הבאים:

6.12.1. על הקבלן לפנות לאבטחת מידע בשינויים המבוצעים במטרה ליישם:

6.12.1.1. שיפורים לרמת השירות המוצע.

6.12.1.2. פיתוח של מערכות ואפליקציות חדשות.

6.12.1.3. שינויים או עדכונים של מסמכי המדיניות ונהלי המשרד.

6.12.1.4. הוספה או שינוי של בקרות במטרה לפתור אירועי אבטחה ולשפר את אבטחת המידע.

6.12.1.5. שינויים והגדלה של רשתות תקשורת.

6.12.1.6. שימוש בטכנולוגיות חדשות.

6.12.1.7. אימוץ של מוצרים חדשים או גרסאות חדשות.

6.12.1.8. סביבות וכלי פיתוח חדשים.

6.12.1.9. שינוי במיקום הפיזי של משרדי הקבלן.

6.12.1.10. שינוי ספקים.

6.12.1.11. תת התקשרות עם קבלן\ספק אחר.

7. בקרה ומעקב

7.1.אבטחת מידע משרד התחבורה תוודא ציות לנוהל זה, בין היתר על ידי כלי ניטור, מעקב וביקורת.

7.2.יתבצע סקר ספק טרם חתימה על ההסכם לוודא עמידה בנהלי אבטחת המידע, כחלק מניהול הסיכונים.

7.3.כל חריגה מנוהל זה מחייבת אישור מראש של אבטחת מידע משרד התחבורה.

7.4.הפרת נוהל זה עלולה להוביל לנקיטת צעדים כנגד הקבלן/ספק בהתאם.

נספח א' - תבנית לדוח ביקורת חצי שנתי :

(הדוח מתייחס לסביבה בה יש מידע של משרד התחבורה בלבד)

1.שם המשרד / העסק / רשות מקומית / הגוף המקבל את המידע.

2.מספר ח.פ.

3.שם הממונה על מאגר המידע (כולל כתובת דוא"ל).

4.שם הממונה בארגון על תחום אבטחת מידע (כולל כתובת דוא"ל).

5.סוג המידע אשר מתקבל ממערכות משרד התחבורה.

6.פירוט ותיעוד של הסמכות לארגון בתחום אבטחת מידע להן ממשק למידע המתקבל ממשרד התחבורה.

7.עמידה בחוק ותקנות הגנת הפרטיות.

8.פירוט מערכות וכלי הגנה וניטור למחשבים אשר בהם נעשה שימוש במערכות של משרד התחבורה.

9.המצאת וסוג מערכת לניטור אירועים חריגים.

10.האם קיים חיבור למרכז ניטור : SOC / SIME , ומה הם נהלי הדיווח.

11.המצאת מערכת הקלטת תקשורת בחיבור למערכות משרד התחבורה.

12.המצאת מערכת / יכולת הלבנה לפני העברת קבצים למשרד התחבורה.

13.שם הגוף / הסמכות אשר מבצעת את הביקורת , כולל פירוט של שם והסמכות מקצועיות של עורך הביקורת.