מדינת ישראל

משרד התחבורה והבטיחות בדרכים

אגף טכנולוגיות דיגיטליות ומידע

הנדון: נספח אבטחת מידע וסייבר למכרז

1. כללי

1.1. מסמך זה כולל אוסף דרישות אבטחת מידע לצורך התקשרות עם הספק.

1.2. עמידה בהוראות מסמך זה מהווה תנאי מהותי להתקשרות עם הספק ועליו לעמוד בדרישות אבטחת המידע וסייבר של המשרד כפי שיעודכנו מעת לעת.

2. מטרה

2.1. הגדרת רמת אבטחת מידע נדרשת כתנאי לאספקת השירותים בהתאם לצרכי המשרד.

3. הגדרות ומושגים

3.1. **מידע:** ידיעה, מסמך, תכתובת, תוכנית, נתון, מודל, חוות דעת, מסקנה וכל דבר אחר הקשור ו/או הנוגע באופן ישיר או עקיף למתן השירותים, לרבות מידע הנוגע לצנעת הפרט של עובדי המשרד או האזרח, בכתובין, בע"פ ו/או בכל צורה או דרך של שימור ידיעות בצורה חשמלית ו/או אלקטרונית ו/או אופטית ו/או מגנטית ו/או אחרת, הקשורים ו/או הנוגעים למתן השירותים ,אשר אינו מצוי בנחלת הכלל.

- שלמות מידע - זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין.
- סודיות המידע – מניעת חשיפת המידע לגורמים לא מורשים.
- זמינות המידע – שמירה על נגישות למידע באופן רציף.
- מידע מוגן - נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.

3.2. **חוק הגנת הפרטיות**: חוק הגנת הפרטיות, התשמ"א – 1981.

3.3. **תקנות הגנת הפרטיות**: תקנות הגנת הפרטיות, התשמ"א – 1981, תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, הנחיות הרשות להגנת הפרטיות וכל תקנות עתידיות שיתוקנו והנחיות עתידיות שיפורסמו בקשר להגנת הפרטיות ואבטחת מידע.

3.4. **מאגר מידע:** אוסף נתוני מידע המוחזק באמצעי מגנטי או אופטי (ובכלל זה מחשב) ומיועד לעיבוד ממוחשב.

3.5. **מנהל המאגר:** מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין.

3.6. **הממונה על אבטחת המידע בצד הספק:** הספק יגדיר איש קשר בעל עולם תוכן טכנולוגי מתאים ורצוי בעל היכרות עם עולם התוכן של איומי הסייבר, אשר יהווה רפרנט אבטחת מידע ליישום ההנחיות המופיעות במסמך זה. פרטיו ודרכי יצירת קשר עמו וזהותו תאושר ע"י משרד התחבורה.

3.7. **נכסי המידע:** כל המידע, מאגרי המידע, נתון אחר או ציוד של המשרד אשר משמש לצורך פעילות המאגר לצורך הפעלת המכרז.

3.8. **מערכות מידע :** כלל הציוד הממוכן התומך בעיבוד והצגת המידע של המשרד הכולל בין השאר: שרתים, מחשבים נייחים וניידים, ציוד תקשורת, ציוד אבטחת מידע ועוד.

3.9. **משתמשי מאגר מידע:**

3.9.1. כל בעל תפקיד אצל הספק, הנדרש מתוקף תפקידו להשתמש במידע אשר נצבר במאגרי המידע של המשרד המצויים אצל הספק, או שיש לספק גישה אליהם.

3.9.2. בעלי תפקידים במשרד המקבלים במסגרת תפקידם דוחות ומידע המופקים ממאגרי מידע של המשרד המצויים בידי הספק או שיש להם גישה אליהם.

3.9.3. מערכות משיקות (צד שלישי) העושות שימוש במידע הנכלל במאגרי המידע של המשרד והמצויים בידי הספק.

3.10. **אבטחה פיזית:** האמצעים הפיזיים הנדרשים להגנה על ציוד המחשוב, לגישה למידע של המשרד ולשרידות המערכות הממוחשבות המכילות את מאגרי המידע.

3.11. **התקן נייד:** מחשב המיועד לשימוש נייד ובכלל זה טלפון נייד כהגדרתו בחוק התקשורת (בזק ושידורים) התשמ"ב-1982 ו\או מצע אחר המשמש לאחסון חומר מחשב/מידע.

3.12. **סיווג מידע:** הקניית הגדרת רגישות למידע ובהתאם את הצורך למדרו, בהתבסס על העקרונות שהוגדרו על ידי המשרד.

3.13. **נזק למידע/איום (Threat)**: פגיעה בסודיות, שלמות וזמינות המידע בבעלותו של המשרד.

3.14. **אבטחת מידע:** הגנה על סודיות, שלמות וזמינות המידע, הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין.

3.15. **אירוע במ"מ/אירוע בטחון מערכות מחשב/אירוע סייבר**: פעולה המתבצעת בזדון או בשוגג העלולה לפגוע בזמינות, אמינות וסודיות המידע ו/או בציוד המחשוב המשרדי ברמות שונות, ולהביא להשבתת מערכות, שיבוש נתונים מכוון או חשיפת נתונים לגורמים לא מורשים.

3.16. **מנגנון הזדהות:** אמצעי המספק פרטים לגבי זהותו של אדם או מערכת בעת ניסיון כניסה ואישור ביצוע פעולות מטעמם למערכת מידע.

3.17. **זיהוי חד ערכי**: ערך ייחודי המזהה את מי שמתיימר להיות בעל אמצעי הזיהוי.

3.18. **הזדהות חזקה**: אמצעי זיהוי המתבסס על לפחות שניים מהפריטים הבאים:

3.18.1. **Something You Are** – תכונה פיזיולוגית ייחודית של המשתמש

3.18.2. **Something You Have** – פריט הנמצא ברשות המשתמש

3.18.3. **Something You Know** – פריט מידע הידוע למשתמש

3.19. **קריפטוגרפיה** :שימוש בכלים מדעיים ואלגוריתמים לצורך הגנה על מידע. המטרות העיקריות של קריפטוגרפיה הינן שמירה על חשאיות ואמינות המידע, מתן פתרון למניעת הכחשה של פעולות ומתן מנגנון לאימות זהות משתמשים.

3.20. **הצפנה**: יישום של קריפטוגרפיה הממירה מידע גלוי (Clear Text) למידע מקודד (Cipher Text) באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים.

3.21. **חומת אש (Firewall)**: רכיב (תוכנה על שרת או רכיב חומרה) המבקר את התעבורה הנכנסת והיוצאת מרשת תקשורת על פי מדיניות אבטחה מוגדרת.

3.22. **פגיעות (Vulnerability)**: חולשה במערכת העלולה להוביל להתממשות איום.

3.23. **לוג (Log): ק**ובץ התיעוד של נתיב בקרה.

3.24. **יה"ב:** היחידה להגנת הסייבר בממשלה – יחידה הפועלת במסגרת רשות התקשוב הממשלתי במשרד הדיגיטל הלאומי. היחידה הוקמה בהתאם להחלטת הממשלה 2443 "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר".

3.25. **מיקור חוץ**: השימוש בשירותי מיקור חוץ משמעו הוצאה מחוץ לארגון, או ביצוע על ידי מי שאינם עובדים בארגון פעולות ותהליכים המבוצעים בדרך כלל על ידי המשרד.

3.26. **ספק:** גורם אשר הוכרז כזוכה במכרז ומעניק שירותים (לרבות יעוץ) או טובין למשרד.

3.27. **ספק מהותי/קריטי** : ספק המספק שירותים כגון : תמיכה ו/או תחזוקת מערכות מידע, אחסון נתונים רגישים מחוץ למשרד, שירותי מיקור חוץ טכנולוגיים או במקרה בו פגיעה בספק עלולה לגרום לנזק מהותי עבור המשרד.

3.28. **ספקים מוסמכים** : ספקים אשר עברו תהליך סקר סיכונים באמצעות בודק וניגשו על ידי בודק לגוף התעדה אשר מורשה להנפיק לספק תעודת "ספק מאושר".

3.29. **מערכת יוב"ל** (יעדים ובקרות לארגון) - מערכת לניהול סיכוני סייבר ואבטחת מידע המהווה פלטפורמה לאומית אשר מורכבת ממספר רכיבים. בין רכיבי המערכת, קיים רכיב אשר מספק מענה לניהול סיכוני הסייבר של שרשרת האספקה בארגון/במשרד הממשלתי. המשרד רשאי לפנות לספק לצורך קבלת ממצאי דו"ח ההתעדה.

3.30. **שאלון ספקים** – שאלון הקיים במערכת יוב"ל או באתר מערך הסייבר הלאומי (קובץ אקסל) שמטרתו לקבוע את רמת הגנת המידע של הספק.

4. <u>השיטה</u>

4.1. הספק ימנה נאמן אבטחת מידע וסייבר, שיהיה אחראי ליישום כלל היבטי אבטחת המידע במערכות ובתהליכים.

4.2. הספק מתחייב לעמוד בדרישות חוק הגנת הפרטיות .

4.3. הספק מתחייב לעמוד בדרישות יה"ב.

4.4. הספק מתחייב לעמוד בדרישות תקני iso בהתאם למכרז בדגש על מידע אישי ורפואי במידה וקיים (iso 27701, 27799) .

4.5. הספק מתחייב ליישם את דרישות "תורת ההגנה בסייבר לארגון" של מערך הסייבר הלאומי ("תורת ההגנה"), באופן שהולם את פעילותו, גודלו ומורכבותו, ותוך ניהול הסיכון כפונקציה של הסתברות והשפעה. תכניות העבודה ליישום הבקרות על-פי תורת ההגנה תאושרנה על-ידי משרד התחבורה.

4.6. בהתאם להחלטת ממשלה 2443, הספק מתחייב לעמוד בתקן ISO27001 למערכת הרלוונטית.

4.7. על הספק להמציא תעודת הסמכה בדבר עמידה בתקן ISO27001 מטעם גוף התעדה, האחראי לבצע מבדק התעדה תחת אקרדיטציה בינלאומית של ANAB

(ANSI National Accreditation Board) כגון : מכון התקנים הישראלי, חברת IQC וכו'. התעודה תומצא למשרד בתוך 120 יום ממועד החתימה על חוזה ההתקשרות.

4.8. הספק מתחייב כי בכל מקרה בו הוא מחזיק ברשומות אשר מכילות מידע אודות כרטיסי אשראי, כהגדרתם בתקן PCI-DSS של חברות האשראי הבין לאומיות, הספק יעמוד בכל הוראות התקן הרלוונטיות לעניין זה ויציג הסמכות בהתאם.

4.9. להלן יפורט אוסף דרישות בתחום אבטחת המידע לצורך התקשרות עם ספק. עמידה בהוראות מסמך זה מהווה תנאי מהותי להתקשרות עם הספק, ועליו לעמוד בדרישות אבטחת המידע של המשרד.

4.10. הכתוב במסמך זה אינו פוטר או גורע מאחריותו של הספק מכל הוראות דין הנוגעות לניהול מאגרי מידע ושמירה על פרטיותו וצנעתו של הפרט או מכל חוק רלוונטי אחר לנושא.

4.11. המסמך אינו מחליף כל הוראה או הנחיה של גורם זה או אחר למול הגוף מקבל המידע, אולם הוא מניח את היסודות שלאורן המשרד מצפה כי הספק ינהג ויישם בעת קבלת מידע ממנו.

4.12. אי יישום העקרונות המובאים במסמך זה בחלקם או במלואם עלול להביא להפסקת ההתקשרות בהתאם לשיקול דעתו המקצועי של המשרד.

4.13.

5. **<u>סיווג ומיפוי המידע</u>**

5.1. הספק יפעל על פי סיווג המידע שהוגדר ע"י המשרד. אפיון השירות יבוצע על פי סיווג זה.

5.2. רגישות מיוחדת תינתן למידע אישי ורפואי במידה וקיים .

6. **<u>אפיון השירות המוצע</u>**

6.1. על הספק לתאר ולצרף מסמך המתאר את מדיניות אבטחת המידע של השירות המוצע.

6.2. הפירוט יכלול בין היתר את הסעיפים הבאים:

- כללי – הסבר כללי על החברה ושיתוף הפעולה עם משרד התחבורה.
- מיקום גאוגרפי בו ממוקמת החברה.
- אבטחה פיזית – לסביבת הפרויקט.
- עץ מבנה ופירוט בעלי תפקידים רלוונטיים (מנכ"ל, מנמ"ר, מנהל אבטחת מידע וכו').
- פירוט הכשרות אבטחת המידע של בעלי תפקידים בתחום אבטחת מידע.
- תיאור התהליך העסקי.
- תיאור ארכיטקטורה של המערכת המוצעת.
- בקרות אבטחת המידע אשר בשימוש המערכת.
- נהלי גיבוי ו-**DR**.
- אופן שילוב תהליך **SDLC** במחזור חיי המערכת.
- תהליכים ארגוניים לצמצום סיכונים והתמודדות עם איומים.
- המצאות והערכה של תאימות לתקינה ולחוקים ופירוט הסמכות לתקני אבטחת מידע: ISO27001, ISO27017 וכו'.
- אופן זיהוי ותגובה לאירועים.
- הערכת עובדים ובדיקות מהימנות.
- ביצוע מבדקי חדירה תקופתיים (מתודה וכו').
- יישום מנגנוני ניטור ובקרה.
- אופן הטיפול בנושא ניהול משתמשים, הזדהות וניהול הרשאות.
- זיהוי חולשות והתקנת טלאים.
- אבטחת מידע בתקשורת (פירוט מוצרים נדרשים).
- בדיקת ממשקים.
- אופן ההגנה על מידע במנוחה ובתנועה.
- מוצרי אבטחת מידע נוספים ברמת התשתית ו/או ברמה האפליקטיבית.
- במידה וספק המערכת מבצע שימוש בתשתית מחשוב של ספק אחר, עליו לציין זאת ולצרף מסמך המתאר כיצד מתבצעת חלוקת האחריות בינו לבין ספק התשתית הנוסף ובאילו אמצעים הוא נוקט בכדי להגן על המידע מפני פגיעות ברמת התשתית ולאשר מול חטיבת אבטחת מידע וסייבר.

7. <u>שמירה על סודיות ופרטיות</u>

7.1. הספק מתחייב לעמוד בהוראות חוק המחשבים, התשנ"ה 1995 – דיני הגנת הפרטיות ובכללם חוק הגנת הפרטיות, התשמ"א 1981 ותקנות הגנת הפרטיות (אבטחת מידע) התשע"ז-2017.

7.2. הספק מתחייב למלא אחר כל הוראות אבטחת המידע לגבי שמירת מידע כפי שיועברו ע"י המשרד.

7.3. הספק ידאג לאבטחת כל חומר שיגיע אליו במסגרת ביצוע התחייבויותיו על פי הסכם זה ויהיה אחראי כלפי המשרד על כל המידע המועבר אליו או דרכו לרבות דוחות, נתונים אישיים, תכתובות דוא"ל, קבצים ,מסמכים ,שרטוטים וכיו"ב על פי ההנחיות שיועברו על ידי המשרד.

7.4. באחריות הספק לדאוג לחיסיון, אמינות וזמינות המידע של המשרד שברשותו.

7.5. בעת אירוע אבטחת מידע/סייבר אצל הספק, לרבות אירוע בו קיים חשד לגבי דלף מידע של המשרד, הספק מחויב להודיע באופן מידי לאיש הקשר מטעם המשרד ולא יאוחר מיום העבודה בו התבצע האירוע והובא לידיעת הספק.

7.6. הספק מתחייב לשתף פעולה עם המשרד בכל אירוע חריג בו מעורב עובד הספק, או שקיים חשד למעורבות שיש עמה השלכה ישירה או עקיפה על ביטחון מערכות המידע של המשרד, בכל הפרה או חשד להפרה של חוקים תקנות או נהלי אבטחת מידע כולל בחקירת אירועים או חשדות לחריגות אבטחת מידע או דליפת מידע של המשרד לגורמים בלתי מורשים.

7.7. ככל שהמסמכים הקשורים לפרויקט, יועברו כשהם מוצפנים, הרי שהמסמכים יישמרו אצל הספק בתצורה מוצפנת.

7.8. מידע "מוגבל" יהיה נגיש לעובדי הספק ע"פ הגדרת הצורך לדעת (Need to Know).

7.9. הכנת עותקים לצרכי עבודה אצל הספק תיעשה על פי צורך בלבד ותפוצתם תהא בקרב עובדי הספק הנדרשים לעותקים אלו בלבד.

7.10. הספק מתחייב למנות ממונה על אבטחת המידע מטעמו, אשר יהיה אחראי על הטיפול במאגרי המידע המצויים בידי הספק וכן על יישום ההנחיות המופיעות במסמך זה.

7.11. הספק יחתום על התחייבות לשמירת סודיות, בנוסח המצורף למכרז, וכן יחתים על התחייבות זו את עובדיו ו/או כל מי מטעמו אשר יהיה בעל גישה למאגר מידע של המשרד או למידע מתוכו במסגרת ההתקשרות.

7.12. הספק מתחייב להפריד הפרדה מלאה ברמה פיזית בין מידע של המשרד שנמצא אצל הספק מתוקף ביצוע המכרז לבין יתר מאגרי המידע שברשותו.

7.13. בכל מקרה שבו לספק התקשרות עם צד שלישי כלשהו אשר יש לו נגיעה עם ההתקשרות בין הספק למשרד במסגרת מכרז זה ו/או על יישום ההנחיות המפורטות במסמך זה, הספק מתחייב לאשר מול המשרד ולפעול על פי הנחיותיו וכן ליידע את הצד השלישי על החובות הנובעים מקיום ההנחיות המפורטות במסמך זה, על הספק לאשר את ההתקשרות עם צד שלישי אל מול המשרד.

8. שימוש, אחזקה וניהול מאגרי מידע

8.1. כל המידע, התוכנות, האפליקציות, הנתונים, קוד וכו' אשר יאוחסנו על ידי הספק יהיו בבעלותו המלאה והבלעדית של המשרד. הספק יצהיר כי הוא מוותר על זכותו לתבוע כל זכות קניינית מהמשרד, ובכלל זה את הזכות לקניין רוחני. למען הסר ספק, כל החומר המועבר על ידי המשרד לספק וכל המידע הנצבר במערכות אשר לספק גישה אליהם הינו בבעלות המשרד כולל זכויות הקניין חומרי ורוחני והינם בבעלותו הבלעדית ואין לספק כל זכות לתבוע שימוש במידע או לבצע בו כל שימוש שאינו באישור המשרד.
הוראה זו לא תחול על מתודולוגיות, נהלי ושיטות עבודה, כלים סטנדרטיים, רעיונות, תפישות, know-how, פיתוחים סטנדרטיים ו/או ידע אשר הינו גנרי ואינו מהווה פיתוח אשר נוצר באופן ייעודי עבור משרד התחבורה – אלה ייחשבו יצירה מוקדמת של הספק ויישארו בבעלותו.

8.2. יובהר כי אין בהוראות המכרז/ההסכם כדי להעביר זכויות יוצרים על מוצרי מדף ו/או מוצרים גנריים של הספק ו/או של צדדים שלישיים (לרבות קוד פתוח) אשר יסופקו /או אשר יעשה בהם שימוש במסגרת מתן השירותים והשימוש של המזמין בהם יהיה כפוף לתנאי הרישיון של היצרן.

8.3. כל שינוי במדיניות הספק בנוגע ליישום ההנחיות במסמך זה יובא לידיעת ואישור המשרד.

8.4. הספק מתחייב שכל גישה שלו, או של מי מטעמו, למידע ולמאגר המידע, תתבצע אך ורק בהתאם להוראות המשרד ולמטרות אשר הוגדרו לו על ידי המשרד במסגרת ההתקשרות.

8.5. הספק מתחייב שהוא, או מי מטעמו, לא יעביר מידע, או חלק ממידע, מתוך מאגרי המשרד אשר בידיו או שיש לו גישה אליהם, לצד שלישי כלשהו ללא אישור מפורש ובכתב מאת המשרד.

8.6. הספק מתחייב למנוע שמירה של נתונים רגישים באופן מקומי אצל משתמשי המערכת. במקרים חריגים יש לקבל אישור מפורש ובכתב מראש מהמשרד.

9. אבטחת המידע במישור משאבי האנוש והעובדים

9.1. הספק מתחייב כי כל עובדיו ו/או מי מטעמו אשר יהיו בעלי גישה למאגרי המשרד ו/או יועסקו במסגרת התקשרות הספק עם המשרד, יהיו בעלי הכשרה מתאימה, בהתאם לנדרש במסמכי המכרז וההתקשרות. בדיקת אימות הרקע של כל מועמד להעסקה כעובד הספק, מי מטעמו או משתמש צד שלישי, יעשו ע"י הספק כנדרש על פי דין ולפי כללי האתיקה הרלוונטיים, והיקפם יתאים לדרישות המשרד, לסיווג המידע שיהיה נגיש להם ולסיכונים הצפויים.

9.2. הספק יהיה אחראי כלפי המשרד על כל פעילות עובדיו ו/או מי מטעמו במסגרת ההתקשרות.

9.3. הספק מתחייב שכל עובדיו, ו/או מי מטעמו ו/או משתמשי צד שלישי, מבינים את מלוא האחריות המוטלת עליהם בנוגע למידע ולאבטחתו וכי הם מתאימים לתפקידים שנועדו להם. על הספק להפחית סיכוני גניבה, הונאה או שימוש לרעה בגישה למידע של המשרד באמצעות נקיטת אמצעי הגנה סבירים ומקובלים (כגון מצלמות אבטחה, תיעוד גישה וכדומה), וזאת מבלי לגרוע מהוראות נספח זה באשר לאבטחה הפיזית והסביבתית.

9.4. על הספק לבצע הדרכות מודעות אבטחת מידע לעובדיו בתחום העיסוק של העובד בתדירות של אחת לשנה ולתעד זאת.

9.5. הספק מתחייב למנוע מקרים בהם עובדיו ו/או מי מטעמו ינסו לבצע גישות למאגרים אליהם לא קיבלו הרשאה.

9.6. הספק מתחייב כי תפקידים ותחומי אחריות של עובדי הספק ו/או מי מטעמו ו/או משתמשי צד שלישי הנוגעים לאבטחה, יוגדרו ויתועדו ע"י הספק לפי מדיניות אבטחת המידע של הארגון.

9.7. חוזה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי אבטחת מידע, וילווה בהצהרה על שמירת סודיות.

9.8. חוזה של הספק עם חברות כוח אדם/השמה או עם חברות המספקות שירותי מיקור חוץ, יכלול התייחסות בכל הנוגע לבדיקות המבוצעות בתהליכי גיוס העובדים. אבטחת מידע בעת העסקת עובדים והגברת המודעות שלהם נוהלי אבטחת מידע של הספק יגדירו מהן הפעולות שיש לבצע בכדי לשמור על נכסי המידע של המשרד.

9.9. על הספק להגדיר נהלים, בקרות ופעולות נוספות המיועדות למנוע את זליגת המידע מעובדים להם יש נגישות למידע של המשרד.

9.10. לעובדים (כולל עובדים חיצוניים לארגון) המסיימים את העסקתם בארגון, בין אם ביוזמתם או ביוזמת המעסיק, ייחסמו הרשאות הגישה למידע (בין אם למערכות מידע ובין אם לאמצעים פיזיים).

9.11. הספק יוודא כי בסיום ההעסקה לא יישארו נכסי מידע של הארגון בידי העובד.

9.12. הספק יגדיר את אופן הטיפול בעובדים בהיבטי אבטחת מידע לתקופת הזמן שבין הודעת העזיבה לסיום העסקה. יש להגדיר דרישות לפחות בנושאי בקרת גישה, עבודה על מערכות ומסמכים וכו'.

10. <u>אבטחה פיזית וסביבתית</u>

10.1. הספק מתחייב לאבטחת אזורי העבודה בהם מתבצע עיבוד מידע השייך למשרד התחבורה.

10.2. בכל מקרה בו מאגר המידע נמצא ברשות הספק, הספק מתחייב לתעד הכנסה והוצאה של ציוד אל המתקנים בהם ממוקם המאגר ומהם.

10.3. הספק מתחייב כי כניסת ספקים או לקוחות לאזורי חוות השרתים תהיה מבוקרת, תכלול ליווי, ותירשם ביומן רישום אירועים.

10.4. הספק מתחייב לכתוב וליישם הנחיות אבטחה פיזית לעבודה באזורים הייעודיים.

10.5. אבטחת ציוד וניירת - הספק יוודא כי הצעדים הבאים ננקטים בכל הנוגע לאבטחת ציוד וניירת:

10.5.1. ציוד המכיל מידע רגיש ומיועד להשמדה או תחזוקה או נמסר אל גורם חיצוני לספק אינו מכיל מידע על לקוחות משרד התחבורה.

10.5.2. מדיית זיכרון שהכילה מידע על לקוחות משרד התחבורה תוצא אל מחוץ לספק לצורכי תחזוקה רק לאחר שננקטו אמצעים מספקים למחיקת המידע באופן המונע אפשרות שחזור המידע באמצעים טכנולוגים גם לאחר מחיקת המידע.

10.5.3. מצעים רגישים אשר אין בהם שימוש ייגרסו או יושמדו.

10.5.4. ניירת המגיעה לסריקה תאובטח באופן נאות, כולל בתהליך הגניזה וההשמדה.

11. <u>אבטחה לוגית</u>

11.1. הספק מתחייב ליישם אמצעי אבטחה הולמים שימנעו חדירה מכוונת או מקרית למערכת או למערכות התשתית והתקשורת, יש להציג את אמצעי הבקרה לחטיבת אבטחת מידע וסייבר טרם יישומם, ולקבל אישור מראש ובכתב על אמצעי הבקרה אותם בחר.

11.2. הספק מתחייב לבצע הפרדה בין רשתות המאכלסות את מאגרי המידע של המשרד ליישומים ולכלל הרשתות (סגמנטציה) באמצעות הפרדה לוגית הכוללת סגמנט מבודד מאחורי חומת אש, יש לפרט את תכנית ההפרדה ולצרף שרטוט רשת.

11.3. הספק מתחייב שכל אמצעי אבטחת המידע יעברו הקשחות לפי המלצות היצרן.

11.4. הספק מתחייב לעדכן באופן שוטף את המערכות השונות למניעת ניצול פרצות אבטחת מידע. עדכונים ברמת חומרה קריטית וגבוהה יותקנו עד 24 שעות לאחר פרסום הודעה ע"י היצרן/משרד/גוף מורשה ממשלתי אחר, עדכונים ברמת חומרה בינונית/נמוכה יותקנו עד שלושה ימי עבודה לאחר פרסום הודעה ע"י היצרן/משרד/גוף מורשה ממשלתי אחר.

1. **<u>אבטחת ענן</u>**:

2. הספק יתחייב להשתמש בטכנולוגיות ענן מאובטחות ומספקות הצפנה הן בעת השמירה על המידע והן בעת העברתו, תוך עמידה בדרישות התקנים והרגולציות הרלוונטיים בתחום האבטחה.

3. הספק מחייב לעמידה בסטנדרט CIS רלוונטי לכל יצרן ענן בהתאם .

4. הספק יוודא שכל ספקי הענן המעורבים בהסכם עומדים בדרישות אבטחת המידע שהוגדרו במסמך זה, כולל הצפנה ברמת מידע במעבר ובמנוחה, ניהול מפתחות הצפנה בצורה מאובטחת, ושימוש במערכות גיבוי מאובטחות.

5. הספק יתבקש להציג את תעודת "הספק מאושר" עבור שירותי הענן, וכן להציג עדכון שוטף של מדיניות אבטחת המידע של ספקי הענן בהתקשרויות עתידיות.

6. הספק יתחייב לבצע סקירות אבטחה שנתיות של מערכות הענן הממוקמות בשירותי הענן, כולל ביצוע בדיקות חדירה ומבצעים אחרים שמטרתן לוודא שהמערכות מעודכנות ועמידות בפני איומים פוטנציאליים.

7. <u>הספק יתחייב להפעיל את שירותי הענן על פי המודלים הבאים:</u>

8. SaaS (Software as a Service): הספק יוודא כי כל המידע הנמצא בשירותי תוכנה המנוהלים בענן יהיה מוצפן הן בעת השמירה והן במהלך העברה, ושהגישה למידע תתבצע רק על פי מדיניות גישה המבוססת על הצורך לדעת (Need to Know).

9. PaaS (Platform as a Service): הספק יתחייב להבטיח שמירה על מערכות הפלטפורמה בענן על ידי שימוש בהגנה על אפליקציות, ביצוע עדכונים שוטפים, ווידוא ניהול הצפנה, מפתחות הצפנה, והגנה מפני התקפות סייבר.

10. IaaS (Infrastructure as a Service): הספק יוודא שמירה על אבטחת המידע בשרתים הווירטואליים, רשתות וירטואליות, ופריטי תשתית אחרים בענן, תוך שימוש באמצעי אבטחה ברמה גבוהה כמו חומות אש (firewalls), הצפנה מלאה של המידע, וכן פתרונות גיבוי מאובטחים.

11. הספק ידרוש מהספקי הענן איתם הוא עובד להציג את תעודת "הספק מאושר" בהתאם להנחיות מערך הסייבר הלאומי, לכל המודלים של שירותי הענן (SaaS, PaaS, IaaS).

12. הספק יוודא שכל הספקים בענן, ללא קשר לסוג השירות (SaaS, PaaS, IaaS), עומדים בדרישות אבטחת המידע שהוגדרו במסמך זה, ומיישמים אמצעי הגנה על המידע במעבר ובמנוחה.

13. הספק יוודא שבסביבות הענן השונות יהיו מנגנוני אבטחה המתאימים לכל אחת מהסביבות:

14. SaaS: הצפנה מלאה של המידע, ניהול גישה מבוקר, ניטור שוטף של פרוטוקולי אבטחת מידע והגנה מפני התקפות כגון פישינג ו- DDoS.
15. PaaS: ניהול והגנה על פלטפורמות פיתוח ויישומים, כולל עדכונים שוטפים של פלטפורמות ותיקוני אבטחה בזמן אמת.
16. IaaS: מנגנוני הגנה ברמות של מערכת הפעלה, וירטואליזציה ורשתות, שמירה על כל תקני האבטחה הגלובליים.
17. הספק ידרוש ביצוע אכיפת מדיניות הצפנה ברמת כל שירות ענן, ויעבוד עם ספקי הענן על מנת לוודא שביצוע הדרישות עומד בתנאי הרגולציה הנדרשים.
18. הספק יוודא שנעשה שימוש בהסכמים חוזיים ברורים עם ספקי הענן, שיכללו התחייבויות של ספקי הענן לעמוד בדרישות אבטחת המידע המוגדרות בסעיף זה.

19. <u>דרישות אבטחת מידע במקרה של ספק:(SaaS (Software as a Service</u>
20. הספק יתחייב לספק שירותי SaaS על פי המודל המאובטח ביותר, תוך הקפדה על:
21. הצפנה מלאה של כל המידע המועבר למערכות הספק וממנו, הן במהלך העברת המידע והן בעת השמירה.
22. הבטחת אבטחת מידע ברמה גבוהה בשרתים שבהם מאוחסן המידע, כולל הצפנה ברמת השכבה, ניהול מפתחות הצפנה, שמירה על זמינות המידע ונגישותם רק למורשים.
23. הספק ידרוש ממערכות ה SaaS-שלו להחיל את מדיניות הצורך לדעת (Need to Know), כלומר, הגבלת גישה למידע רק לעובדים או גורמים שיש להם צורך ישיר במידע לשם ביצוע תפקידם.
24. הספק יוודא כי ישנם אמצעי זיהוי חזקים (MFA) עבור הגישה לשירותי ה SaaS-, ויישום אמצעי בקרת גישה נוספים המבוססים על תפקידים כדי למנוע גישה לא מורשית.
25. הספק יתחייב לבצע עדכונים שוטפים לאפליקציות ה SaaS-, כולל תיקוני אבטחה שוטפים, ועדכון תוכנות ככל שמופיעים פגיעויות חדשות או התקפות סייבר שזוהו.
26. הספק יתחייב לבצע אכיפה של מדיניות אבטחה פנימית עבור שירותי ה SaaS-, כולל ביצוע ביקורות סדירות של מערכות, ביצוע בדיקות חדירה (penetration tests) כדי לזהות פרצות אבטחה פוטנציאליות, ושיפור מתמיד של מערכות האבטחה של ה.SaaS-
27. הספק יתחייב לספק דוחות אבטחת מידע שוטפים למשרד, ויהיה אחראי לדיווח על התראות מיידיות במקרה של אירועים אבטחתיים (כגון דלף מידע, ניסיון חדירה וכו').
28. הספק יוודא כי לכל מגע עם צדדים שלישיים או ספקי משנה במסגרת שירותי ה SaaS-, יהיו הסכמים ותנאים שמחייבים את אותם צדדים להחיל את אותן דרישות אבטחת מידע כפי שמוגדרות בסעיף זה.
29. הספק יתחייב למנוע שמירה של מידע רגיש על תחנות קצה של משתמשי SaaS, אלא אם כן הדבר דרוש לתפקודו של המשתמש ועם אישור מראש מהמשרד. במקרה כזה, המידע יאוחסן בצורה מוצפנת.

12. <u>ניהול משתמשים והרשאות</u>

12.1. הספק מתחייב שגישה למערכות המידע ו/או מאגרי המידע תתבסס על הצורך לדעת (need to know) ולא תורשה גישה מעבר לנדרש לצורך מילוי התפקיד כפי שהוגדר על ידי המשרד ובהתאם להוראות המכרז.

12.2. הספק מתחייב לדאוג לגישה ממודרת על בסיס הגדרת תפקידים.

12.3. הספק מתחייב לנהל רישום מעודכן של בעלי התפקידים ושל הגישה המוגדרת לכל תפקיד.

12.4. הספק מתחייב לגרוע הרשאות לבעלי תפקידים שהסתיים תפקידם או שאין להם צורך במידע אליו קיבלו הרשאה.

12.5. הספק מתחייב לדאוג לבקרות המתאימות על מנת שלא תבוצע גישה לא מורשית למאגרי המידע, יש לצרף למענה את הפתרון לדרישה.

12.6. הספק מתחייב שהזדהות לניהול הרשת והשירותים הניהוליים מרחוק תבוצע באמצעות רכיב פיסי בנוסף לסיסמה (2FA).

12.7. על הספק לזהות את המשתמשים במערכות שבמכרז, מערך ההזדהות תוגדר מדיניות סיסמאות שתכלול את הפרמטרים הבאים לכל הפחות:

12.7.1. חוזק הסיסמה - לפחות 10 תווים בשילוב של ספרות ואותיות

12.7.2. מספר ניסיונות שגויים לנעילה - 5 ניסיונות

12.7.3. שמירת היסטורית סיסמאות - עד 5 סיסמאות אחורה

12.7.4. תדירות החלפת הסיסמה - אחת ל-3 חודשים

12.8. הספק מתחייב לנתק משתמש שהזדהה למערכת מידע לאחר פרק זמן של 10 דקות ללא פעילות.

13. <u>אבטחת רכיבי תקשורת</u>

13.1. הספק מתחייב כי מערכות ומאגרי המידע של המשרד לא יחוברו לסביבת האינטרנט, אלא אם כן קיבל את אישור המשרד לכך מראש ובכתב.

13.2. במידה וקיבל הספק אישור וחיבר את המערכות ו/או מאגרי המידע לרשת ציבורית או לאינטרנט, מתחייב הספק לנקוט באמצעי ההגנה המתאימים על מנת למנוע נזק, פריצה, זיהום או השחתה של מאגרי המידע, יש לפרט את הצעת הספק להתמודד עם האיומים הנ"ל ולצרף למענה את רשימת הבקרות והאמצעים הנותנים מענה לדרישה.

13.3. הספק מתחייב שהעברת המידע בתוך רשת התקשורת, ברשת ציבורית או על גבי רשת האינטרנט תיעשה תוך שימוש בשיטות הצפנה מקובלות בפרוטוקולים מתקדמים.

13.4. על ציוד הקצה המשמש להעברת תקשורת (מתגים, נתבים, FW) לעבור הקשחות בהתאם למדיניות היצרן ולעבור עדכוני קושחה.

14. <u>אבטחת עמדות הקצה</u>

14.1. חל איסור מוחלט לשמור מידע רגיש בתחנה מרוחקת של המשתמש שלא הותאמה למדיניות מסמך זה.

14.2. מחשבי הספק מהם ניתן לגשת למידע של המשרד ולמערכותיו, יצוידו במערכת הפעלה ובתוכנות אנטי וירוס מעודכנות לצורך הגנה מפני קוד זדוני (וירוסים, תולעים, סוסים טרוייאנים ותוכנות רוגלה אחרות).

14.3. העברת מידע לרשת המשרד תבוצע לאחר תהליך הלבנה.

14.4. הסביבה שתוגדר לצורך טיפול במידע של המשרד תופרד מסביבת העבודה של הספק באמצעות אמצעים לוגיים (FW, סגמנטציה) או ע"י הפרדה פיזית מלאה.

14.5. דוחות אירועי מערכת של תחנות העבודה יועברו למערכות הניטור של הספק.

15. <u>שימוש בהתקנים ניידים</u>

15.1. הספק מתחייב שלא להוציא חלקי מידע להתקנים ניידים למעט גיבוי המידע כפי שנקבע על ידי המשרד.

15.2. במידה ונדרש מהספק לצורך פעילותו לבצע העלאת חלקי מידע לצורך גיבוי, מתחייב הספק לפנות לקבלת אישור מראש של חטיבת אבטחת המידע וסייבר במשרד וכן לנקוט באמצעי הגנה נאותים על מנת להבטיח את שלמות, סודיות וזמינות המידע.

15.3. במידה ונדרש מהספק לצורך פעילותו לבצע העלאת חלקי מידע לקלטת גיבוי מתחייב הספק לוודא כי אין ערוב של מידע מסיווגים שונים על אותו התקן.

16. <u>סיום התקשרות</u>

16.1. המשרד ידרוש מהספק את מחיקת המידע בסיום ההתקשרות, או בכל נקודת זמן שקודמת לה (לדוגמה במקרה של חשד לפריצה ו/או דלף מידע אצל הספק).

16.2. יש לוודא כי הסדרים עם הספק שנקבעו במסגרת הסכם ההתקשרות, מתקיימים. בפרט חשוב לוודא עמידה בכל הקשור למחיקת נתונים של המשרד המאוחסנים בחצרי הספק בתום ההתקשרות בין הצדדים. בין היתר יש לבדוק את הנושאים הבאים:

- יש לוודא החזרת כלל הרשומות, המדיה, הציוד והרכיבים השייכים למשרד אשר נעשה בהם שימוש לצורך עבודת הספק. כל זאת, לרבות פריטים הנמצאים בקרב כלל עובדי הספק וספקי המשנה שלו.
- ספק העובד בסביבת ענן יוודא מחיקת החומר ומחיקת מפתח ההצפנה על מנת לוודא כי חומר שנשאר אינו קריא.
- הספק יחתום על הצהרה בה הוא מתחייב שלא נשארו ברשותו רכיבים כלשהם הנוגעים למערכת ו/או מידע אודות המשרד וכי הוא לא יעשה שום שימוש במידע על המשרד, אליו הוא נחשף במסגרת ההתקשרות.
- יש לוודא השמדת מדיה מגנטית מכל ציוד אשר שימש את הספק במהלך ההתקשרות עם המשרד (כגון: במקרה שמדובר במחשבים של הספק ששימשו לעיבוד ו/אחסון של מידע של המשרד). כמו כן, נדרש לוודא מחיקת עותקים של קבצים ומידע של הלקוח ממערכות המידע ונכסי ה-**IT** של הספקים לאחר סיום הצורך העסקי באחזקתו. המחיקה תתבצע בהתאם לנוהל המופיע **<u>בקישור הבא</u>**.
- יש לוודא כי לספק לא נותרות הרשאות גישה, אמצעי הזדהות וגישה פיזית ו/או לוגית למידע של המשרד.
- יש לוודא הנחיה לעניין המותר והאסור אודות פרסום פרטי הפרויקט/התקשרות לגורמי צד ג'.

מ ד י נ ת י ש ר א ל

משרד התחבורה
והבטיחות בדרכים

אגף טכנולוגיות דיגיטליות ומידע

<u>נספח שמירת סודיות</u>

אני _____ ת"ז _____ עובד בחברה/גוף/עסק _____ (להלן – "המציע") או מועסק על ידה, מצהיר ומתחייב בזה, כלפי ממשלת ישראל וכלפי המציע:

1. לא לגלות, להראות או למסור, בין במשך תקופת העסקתי בחברה ו/או על ידה ובין לאחר מכן, לשום אדם או גוף, שום סודות מסחריים, ו/או אחרים של ממשלת ישראל ו/או של המציע ושום מידע הנוגע לממשלה ו/או למציע בכלל ולעניין הסכם ההתקשרות עם משרד התחבורה והבטיחות בדרכים במסגרת מכרז מספר_____(להלן - "ההסכם") בפרט, או שום מידע הקשור במישרין או בעקיפין, ברכושם, עסקיהם, ענייניהם, לקוחותיהם, ספקיהם והאנשים או הגופים הקשורים בממשלה ו/או במציע או הבאים עימם במגע לרבות, אך מבלי לגרוע מכלליות האמור לעיל, נושאי מחקר ופיתוח של הממשלה ו/או המציע, שיטות יצור, תהליכים, מחירים, תחשיבים, תנאי התקשרות עם לקוחות וספקים, שרטוטים מסמכים וסודות מקצועיים*, וזאת בין שהסודות והאינפורמציה האמורים הגיעו אלי כתוצאה מהעסקתי במציע ו/או במתן שירותים לממשלה ובין שהגיעו לידיעתי בכל אופן אחר שהוא;
2. לא לעשות כל שימוש במידע כאמור לעיל שלא למטרות ביצוע השירותים נשוא מכרז זה, כולל בצוע שכפולים, העתקים וכיו"ב;
3. ידוע לי כי אי מילוי ההתחייבויות כלפי הממשלה על פי הצהרה זו מהווה עבירה על חוק העונשין, התשל"ז – 1977;
4. ידוע לי שהעברת מידע כאמור בסעיף 1 ו/או או 2 לעיל, למאן דהו, ללא אישור בכתב ומראש מהממשלה, עלול להסב לממשלה נזקים כלכליים משמעותיים ביותר;
5. התחייבות זו תמשיך לחול אף לאחר תום תקופת ההסכם האמור. התחייבות זו לא תחול על מידע שהוא בבחינת נחלת הציבור.

שם הספק: _____

פרטי מורשה חתימה: _____

שם מלא: _____ תפקיד: _____ חתימה +חותמת _____

*"**סודות מקצועיים**" - כל מידע אשר יגיע לידי הספק, בין אם נתקבל במהלך מתן השירותים או לאחר מכן, לרבות ומבלי לפגוע בכלליות האמור לעיל: מידע אשר יימסר ע"י המשרד התחבורה ו/או כל גורם אחר ו/או מי מטעמו.