

נספח טז' 4 - דרישות אבטחת מידע

הנדון: נספח אבטחת מידע למכרז במכרז בקרה על רכבת ישראל

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 ששנו, 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 ניידים 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 המחשב, 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 כדן.
- 3.15. **אירוע במ"מ/אירוע בטחון מערכות מחשב/אירוע סייבר:** פעולה המתבצעת בזדון או בשוגג העלולה לפגוע בזמינות, אמינות וסודיות המידע ו/או בצידוד 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 מטעמים 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):** קובץ 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".

4. השיטה

- 4.1. הספק ימנה נאמן אבטחת מידע וסייבר, שיהיה אחראי ליישום כלל היבטי אבטחת המידע במערכות ובתהליכים.
- 4.2. בהתאם להחלטת ממשלה 2443, הספק מתחייב לעמוד בתקן ISO27001 למערכת הרלוונטית תוך 90 יום מרגע הזכייה במכרז.
- 4.3. 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'.
- 4.4. התעודה תומצא למשרד בתוך 120 יום ממועד החתימה על חוזה ההתקשרות. הספק מתחייב לעמוד בתקן ISO27017 לעבודה בסביבות הענן במידה ומתקיימת עבודה בסביבה זו.
- 4.5. 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.
- 4.6. 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.
- 4.7. 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.

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

5. סיווג ומיפוי המידע

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

6. אפיון השירות המוצע

6.1. על הספק לתאר ולצרף מסמך המתאר את מדיניות אבטחת המידע של השירות המוצע.
6.2. 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. שמירה על סודיות ופרטיות

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. הספק יהיה אחראי לכל עקיפה או ניסיון עקיפת מנגנוני אבטחה ובקורות גישה לתשתיות שונות, שיבוצע על ידי מי מהעובדים מטעמו.

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

7.7. 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.

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

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

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

7.11. על הספק ליישם יכולת הגדרה במערכי הניטור לרישום גישה או ניסיונות גישה למידע המוגדר כרגיש.

7.12. 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.

7.13. 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.

7.14. הספק מתחייב להפריד הפרדה מלאה את מאגרי/נכסי המשרד המצויים בידיו ברמה פיזית מיתר מאגרי המידע שברשותו.

7.15. 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 ליידיע את הצד השלישי על החובות הנובעים מקיום ההנחיות המפורטות במסמך זה, על הספק לאשר את ההתקשרות עם צד שלישי אל מול המשרד.

7.16. המשרד רשאי לבצע בקרה תהליכית וטכנולוגית אצל הספק, לאחר תיאום עמו לפחות שבוע טרם ביצוע הבקרה. הספק מתחייב לשתף פעולה עם נציגי המשרד לצורך כך.

7.16.1. הספק יספק למשרד את הפרטים הנדרשים לבקרה: בעלי תפקידים רלוונטיים לאבטחת מידע, פרטי ספקי מערכות קריטיות ושירותים (ספק ענן, ספק אינטרנט, אירוח אתרי אינטרנט וכדומה). הספק יעדכן את המשרד התחבורה בכל שינוי בפרטים אלה.

7.17. בקרות אירוע אבטחת מידע אצל הספק, תאושר גישה לעובדי המשרד או מי מטעמו לכלל מערכות המידע הרלוונטיות לאירוע.

8. שימוש, אחזקה וניהול מאגרי מידע

- 8.1. כל המידע, הנתונים, 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.
- 8.2. כל שינוי במדיניות הספק בנוגע ליישום ההנחיות במסמך זה יובא לידיעת ואישור המשרד.
- 8.3. 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.
- 8.4. 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.
- 8.5. 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 סיכונים 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, בקורות 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 יודא 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. אבטחה פיזית וסביבתית

- 10.1. הספק מתחייב לאבטחת אזורי העבודה בהם מתבצע חיבור למשרד התחבורה ובכלל זה עבודה על מערכות/מאגרי מידע של המשרד.
- 10.2. הספק מתחייב כי הגישה לאזורים שקיים בהם מידע ו/או מאגרי מידע וארונות התקשורת תהיה מתועדת ומבוקרת באופן המאפשר את וידוא זהות האדם הניגש לציד הנ"ל.
- 10.3. בכל מקרה בו מאגר המידע נמצא ברשות הספק, הספק מתחייב לתעד הכנסה והוצאה של ציוד אל המתקנים בהם ממוקם המאגר ומהם.
- 10.4. הספק מתחייב כי כניסת ספקים או לקוחות לאזורי חוות השרתים תהיה מבוקרת, תכלול ליווי, ותירשם ביומן רישום אירועים.
- 10.5. אמצעים לבקרת כניסה פיזית: הספק מתחייב כי השרתים והציוד המשמש לאחסון, עיבוד וגישה למאגרי המידע והיישומים יוגנו על ידי אמצעים מתאימים לבקרת כניסה כדי להבטיח שרק לעובדים מורשים תותר הגישה.
- 10.6. הספק מתחייב לכתוב וליישם הנחיות אבטחה פיזית לעבודה באזורים הייעודיים.
- 10.7. אבטחת ציוד וניירת - הספק יודא כי הצעדים הבאים ננקטים בכל הנוגע לאבטחת ציוד וניירת:
 - 10.7.1. ציוד המכיל מידע רגיש ומיועד להשמדה או תחזוקה או נמסר אל גורם חיצוני לספק אינו מכיל מידע על משרד התחבורה.
 - 10.7.2. 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 טכנולוגיים גם לאחר מחיקת המידע.
 - 10.7.3. מצעים רגישים אשר אין בהם שימוש ייגרסו או יושמדו.
 - 10.7.4. ניירת המגיעה לסריקה תאובטח באופן נאות, כולל בתהליך הגניזה וההשמדה.

11. אבטחה לוגית

- 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 שכל אמצעי אבטחת המידע יעברו הקשחות לפי המלצות היצרן.

12. ניהול משתמשים והרשאות

- 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 לדאוג לבקורות המתאימות על מנת שלא תבוצע גישה לא מורשית למאגרי המידע.

13. אבטחת עמדות הקצה

- 13.1. חל איסור מוחלט לשמור מידע רגיש בתחנה מרוחקת של המשתמש שלא הותאמה למדיניות מסמך זה.
- 13.2. מחשבי הספק מהם ניתן לגשת למידע של המשרד ולמערכותיו, יצוידו במערכת הפעלה ובתוכנות אנטי וירוס מעודכנות לצורך הגנה מפני קוד זדוני (וירוסים, תולעים, סוסים טרויאניים ותוכנות רוגלה אחרות).
- 13.3. הספק מתחייב לא לשמור מידע של משרד התחבורה על מחשבים ניידים ו/או טלפונים חכמים.
- 13.4. העברת מידע לרשת המשרד תבוצע לאחר תהליך הלבנה.
- 13.5. דוחות אירועי מערכת של תחנות העבודה יועברו למערכות הניטור של הספק.
- 13.6. החיבור אל מערכות המידע של המשרד יהיה בהתאם להנחיות המשרד.

14. שימוש בהתקנים ניידים

- 14.1. הספק מתחייב שלא להוציא חלקי מידע להתקנים ניידים למעט גיבוי המידע כפי שנקבע על ידי המשרד.
- 14.2. 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.

- 14.3. במידה ונדרש מהספק לצורך פעילותו לבצע העלאת חלקי מידע לקלטת גיבוי מתחייב הספק לוודא כי אין ערוב של מידע מסיווגים שונים על אותו התקן.
- 14.4. במאגר מידע שניתן להתחבר אליו מרחוק באמצעות רשת האינטרנט למטרות ניהול, הספק מתחייב לבצע הזדהות חזקה (MFA).

15. פיקוח וביקורות תקופתיות

- 15.1. כאמור בסעיף 9 לעיל (זיהוי וניהול סיכונים), הספק מתחייב לבצע סקר אבטחת מידע (Security Audit) לפחות אחת ל-36 חודשים ותיקוף לסקר אחת ל-18 חודשים. בנוסף, מתחייב הספק לבצע כל 18 חודשים מבדק חדירה (Penetration Test) לרשת התקשורת שלו ולמערכות שלו על ידי צד שלישי שזהותו אושרה על ידי משרד התחבורה, ולהעביר את ממצאי הסקר ומבדק החדירה לעיונו של מנהל אבטחת מידע של המשרד.
- 15.2. המשרד רשאי לערוך ביקורות (באמצעות מחלקת אבטחת מידע של המשרד ו/או ע"י ספק חיצוני המועסק מטעמו) בחצרי או במערכות הספק (מעבר לאלה שתערוך חברת אבטחת המידע בה יבחר הספק) לשם ווידוא עמידה בהנחיות מסמך זה ו/או לצורך זיהוי כל סיכון אפשרי על המידע של המשרד. ביקורות אלו עשויות לכלול, על פי שיקול דעתו של המשרד, את אלה:
- 15.2.1. בקרה על תהליכי ונהלי עבודה רלוונטיים לעבודת הספק מול המשרד;
- 15.2.2. יישום אמצעי אבטחת המשאב האנושי בחצרות הספק;
- 15.2.3. יישום אמצעי אבטחה פיזית וסביבתית בחצרות הספק;
- 15.2.4. יישום אמצעי אבטחה לוגית בחצרות הספק (כולל כניסה למערכות הספק ו/או בדיקה באמצעות כלים ממוכנים ברשת ומערכות הספק);
- 15.2.5. בחינת חוסן מערכות המידע של הספק מתוך או מחוץ לרשת הספק על ידי גורם חיצוני בלתי תלוי, כפי שיוגדר על ידי המשרד (תוך תיאום עם הספק ובהסכמתו).

16. סיום התקשרות

- 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 תבצע בהתאם לנוהל המופיע ב**קישור הבא**.
 - 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'.

נספח שמירת סודיות

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 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.