



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 ששוננו, 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.



אגף טכנולוגיות דיגיטליות ומידע

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 ושירותים) 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 מטעם 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 התייעוד 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.



אגף טכנולוגיות דיגיטליות ומידע

- 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 ובקורות 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. השיטה

- 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 הבקורות 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 ויצגי 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.



אגף טכנולוגיות דיגיטליות ומידע

5. סיווג ומיפוי המידע

- 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. אפיון השירות המוצע

- 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.
 - בקורות 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.



אגף טכנולוגיות דיגיטליות ומידע

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. בעת אירוע אבטחת מידע/סייבר או אירוע חריג 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. על הספק ליישם יכולת הגדרה במערכי הניטור לרישום גישה או ניסיונות גישה למידע המוגדר כרגיש.
- 7.11. 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.
- 7.12. 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.
- 7.13. הספק מתחייב להפריד הפרדה מלאה את מאגרי המשרד המצויים בידי ברמה פיזית מיתר מאגרי המידע שברשותו.
- 7.14. 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.
- 7.15. 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.
 - 7.15.1. 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.



אגף טכנולוגיות דיגיטליות ומידע

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.
- 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. זיהוי וניהול סיכונים

- 9.1 על הספק לפרט תכנית ביצוע לניהול וזיהוי סיכונים אבטחת מידע בכל שלב משלבי הפרויקט.
- 9.2 הספק יבצע סקרי סיכונים אבטחת מידע וסייבר תקופתיים למוצרי אבטחה, מערכות, תשתיות ותהליכים מרכזיים. ביצוע סקר הסיכונים, לא יפחת מאחת ל-36 חודשים ויתוקף לפחות אחת ל-18 חודשים. הסקרים יבוצעו על-ידי חברה חיצונית, המתמחה בנושא אבטחת מידע וסייבר, ושאינה קשורה לספק או לגופים שפיתחו את המערכות. ממצאי הסקרים יוצגו לחטיבת אבטחת מידע וסייבר במשרד התחבורה, ותכנית עבודה לתיקונים תגובש על פי תעדוף של משרד התחבורה. הספק מתחייב לפעול בהתאם לתוכנית העבודה לתיקונים של סיכונים אבטחת המידע שהתגלו.
- 9.3 הספק מתחייב לפנות למשרד בבקשה לאישור לפני ביצוע שינויים בארכיטקטורת המערכת, או באופן מתן השירותים. הספק מתחייב שלא לבצע שינוי כלשהו ללא אישור מפורש ובכתב מהמשרד.
- 9.4 הספק רשאי להציע בקרות חלופיות לדרישות המפורטות במסמך זה, בקרות אלו ייושמו לאחר קבלת אישור מראש בכתב של גורמי אבטחת המידע במשרד.

10. אבטחת המידע במישור משאבי האנוש והעובדים

- 10.1 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, לסיוג המידע שיהיה נגיש להם ולסיכונים הצפויים.
- 10.2 הספק יהיה אחראי כלפי המשרד על כל פעילות עובדיו ו/או מי מטעמו במסגרת ההתקשרות.



אגף טכנולוגיות דיגיטליות ומידע

- 10.3. 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.
- 10.4. על הספק לבצע הדרכות מודעות אבטחת מידע לעובדיו בתחום העיסוק של העובד בתדירות של אחת לשנה ולתעד זאת.
- 10.5. הספק מתחייב למנוע מקרים בהם עובדיו ו/או מי מטעמו ינסו לבצע גישות למאגרים אליהם לא קיבלו הרשאה.
- 10.6. 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.
- 10.7. חוזה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי אבטחת מידע, וילווה בהצהרה על שמירת סודיות.
- 10.8. 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.
- 10.9. על הספק להגדיר נהלים, בקורות ופעולות נוספות המיועדות למנוע את זליגת המידע מעובדים להם יש נגישות למידע של המשרד.
- 10.10. 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).
- 10.11. הספק יודא כי בסיום ההעסקה לא יישארו נכסי מידע של הארגון בידי העובד.
- 10.12. 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'.

11. אבטחה פיזית וסביבתית

- 11.1. הספק מתחייב לאבטחת אזורי העבודה בהם מתבצע עיבוד מידע השייך למשרד התחבורה.
- 11.2. בכל מקרה בו מאגר המידע נמצא ברשות הספק, הספק מתחייב לתעד הכנסה והוצאה של ציוד אל המתקנים בהם ממוקם המאגר ומהם.
- 11.3. הספק מתחייב כי כניסת ספקים או לקוחות לאזורי חוות השרתים תהיה מבוקרת, תכלול ליווי, ותירשם ביומן רישום אירועים.
- 11.4. הספק מתחייב לכתוב וליישם הנחיות אבטחה פיזית לעבודה באזורים הייעודיים.
- 11.5. אבטחת ציוד וניירת - הספק יודא כי הצעדים הבאים ננקטים בכל הנוגע לאבטחת ציוד וניירת:
 - 11.5.1. ציוד המכיל מידע רגיש ומיועד להשמדה או תחזוקה או נמסר אל גורם חיצוני לספק אינו מכיל מידע על לקוחות משרד התחבורה.
 - 11.5.2. 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 טכנולוגיים גם לאחר מחיקת המידע.
 - 11.5.3. מצעים רגישים אשר אין בהם שימוש ייגרסו או יושמדו.
 - 11.5.4. ניירת המגיעה לסריקה תאובטח באופן נאות, כולל בתהליך הגניזה וההשמדה.



אגף טכנולוגיות דיגיטליות ומידע

12. אבטחה לוגית

- 12.1. 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 יישום, ולקבל אישור מראש ובכתב על אמצעי הבקרה אותם בחר.
 - 12.2. 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.
 - 12.3. הספק מתחייב שכל אמצעי אבטחת המידע יעברו הקשחות לפי המלצות היצרן.
 - 12.4. הספק מתחייב לעדכן באופן שוטף את המערכות השונות למניעת ניצול פרוצדורות 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. **אבטחת ענן :**
 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. **הספק יתחייב להפעיל את שירותי הענן על פי המודלים הבאים:**
 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:



אגף טכנולוגיות דיגיטליות ומידע

- 14. SaaS : הצפנה מלאה של המידע, ניהול גישה מבוקר, ניטור שוטף של פרוטוקולי אבטחת מידע והגנה מפני התקפות כגון פשינג 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. דרישות אבטחת מידע במקרה של ספק: SaaS (Software as a Service)
- 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.

13. תיעוד ובקרה

- 13.1. הספק מתחייב לנהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת על כלל המערכות הטכנולוגיות, בכלל זה הכוונה גם למאגרי מידע של המשרד.
- 13.2. הספק יישם מנגנוני בקרה Audit על ממשקי ניהול של מערכות הגנה, תשתיות, ממשקים ומערכות מרכזיות, לצורך זיהוי והתרעה על אירועי אבטחה חריגים, הן מצד משתמשים פנימיים והן מצד משתמשים חיצוניים. יש לצרף למענה את הפתרון לדרישה.



אגף טכנולוגיות דיגיטליות ומידע

- 13.3. על הספק לבצע תיעוד של כל אירוע אשר יש בו משום פגיעה בשלמות, סודיות וזמינות המידע, יש לצרף למענה את הפתרון לדרישה.
- 13.4. כל אירוע אבטחה, ייחקר וייבדק ויופק דוח אירוע המתאר את הגורמים לאירוע ואת דרכי הטיפול באירוע. הספק יוציא הנחיות לביצוע על מנת להפחית את הסיכוי לאירוע דומה. בנוסף, הספק יעביר את דוח האירוע לעיון חטיבת אבטחת מידע וסייבר של משרד התחבורה.
- 13.5. על הספק להכין הוראות להתמודדות עם אירועי אבטחת מידע אשר מתייחסים לחומרת האירוע ולמידת רגישות המידע. בהוראות אלו תהיה התייחסות לצעדים מידיים הנדרשים לטיפול באירוע כגון דיווח למשרד, ביטול הרשאות וכדומה, יש לצרף למענה דוגמא לדרישה.
- 13.6. הספק ישלב פתרון לתיעוד פעילות אשר תוגדר קריטית במערכת, פעילות אשר נראית חריגה (כולל פעילות בבסיס הנתונים ו/או במערכת ההפעלה), ופעילות או ניסיונות לביצוע פעולות אשר נוגדת ישירות את המדיניות שהוגדרה במערכת. כמו כן, על המערכת לספק כלים מתאימים לשמירה על קבצים אלו ויכולות דיווח לבעלי התפקידים המתאימים כדי שיוכלו לטפל בהתערות.
- 13.7. מנגנון הבקרה במערכות יאפשר ביצוע מעקב אחר האירועים הבאים:
- שימוש במנגנון ההזדהות – Login\Logout.
 - ניסיון כושל בכניסה למערכת.
 - ניסיונות גישה למידע ללא הרשאת גישה.
 - אירועים אפליקטיביים שיוגדרו כדורשי בקרה עפ"י מנגנון כללים מיוחד לנושא.
 - מחיקת אובייקטים במערכת.
 - פעילויות המבוצעות על-ידי גורמים בעלי הרשאות גבוהות.
 - פעולות אדמיניסטרציה (ניהול משתמשים, הורדה והעלאת Services וכו').
 - שגיאות תפעוליות (נפילת מערכת, הודעות שגיאות תוכנה וכו').
- 13.8. עבור כל אירוע המוגדר כדורש בקרה יישמרו הפרטים הבאים:
- תאריך ושעה.
 - מקור ביצוע הפעולה לדוגמה: כתובת IP\DOMAIN.
 - שם המשתמש.
 - סוג האירוע.
 - הצלחה או כישלון של האירוע.
 - זיהוי האובייקט עליו מבוצעת הפעולה לדוגמא: שם קובץ.
 - תיאור הפעולה (מה בוצע): עבור כל סוג אירוע יש לספק תוכן רלוונטי. למשל: עדכון רשומה, ניסיון גישה לרשומה, מחיקת משתמש, הורדת מערכת וכו'.
 - על ההודעות צריכות להיות אמינות, מלאות וברורות.
 - על הספק לפרט יכולות המערכת לייצא את הנתונים לקונסולה מרכזית (מערכת שו"ב).
 - על מנגנון הבקרה להתממשק למנגנון הדוחות ולספק רמה גבוהה של דוחות, חיתוך מידע, וכו'.
 - על הספק לפרט יכולות דיווח של המערכת (בדוא"ל, SMS וכו') למנהלי המערכת על אירועים שיוגדרו כך.



אגף טכנולוגיות דיגיטליות ומידע

- על מערך הבקרה להיות מאובטח כראות. רק משתמשים מורשים יקבלו גישה אליו, ובמיוחד יש להקפיד על בקרת גישה ליכולת להעלות ולהוריד את מנגנון הבקרה.

- 13.9. הספק מתחייב שתיעוד הגישה ישמר בשרתים נפרדים ממאגר המידע.
- 13.10. הספק מתחייב כי מנגנון הבקרה לא יאפשר, ביטול או שינוי של הפעלתו. מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראי אבטחת מידע מטעם הספק ולחטיבת אבטחת מידע וסייבר במשרד.
- 13.11. הספק מתחייב להעביר למשרד דיווחים תקופתיים ולפי דרישה בכל הנוגע לאופן ניהול מידע, אשר נמצא בבעלות המשרד ובעת אירועי סייבר.
- 13.12. הספק מתחייב להגיש למשרד כל שנה דו"ח ביקורת חיצוני חתום ע"י גורם מוסמך ומקצועי (כל גורם המלווה ארגונים להסמכות אבטחת מידע).
- 13.13. הספק מתחייב לדווח באופן מידי לחטיבת אבטחת מידע וסייבר במשרד בכל מקרה של ארוע סייבר, חשש לדליפת מידע מהמאגר או שימוש חורג מההרשאה שניתנה.
- 13.14. הספק מתחייב לשמור את נתוני הרישום של מנגנון הבקרה למשך 24 חודשים לפחות.

14. ניהול משתמשים והרשאות

- 14.1. 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.
- 14.2. הספק מתחייב לדאוג לגישה ממודרת על בסיס הגדרת תפקידים.
- 14.3. הספק מתחייב לנהל רישום מעודכן של בעלי התפקידים ושל הגישה המוגדרת לכל תפקיד.
- 14.4. הספק מתחייב לגרוע הרשאות לבעלי תפקידים שהסתיים תפקידם או שאין להם צורך במידע אליו קיבלו הרשאה.
- 14.5. הספק מתחייב לדאוג לבקרות המתאימות על מנת שלא תבוצע גישה לא מורשית למאגרי המידע, יש לצרף למענה את הפתרון לדרישה.
- 14.6. הספק מתחייב שהזדהות לניהול הרשת והשירותים הניהוליים מרחוק תבוצע באמצעות רכיב פיסי בנוסף לסיסמה (2FA).
- 14.7. על הספק לזהות את המשתמשים במערכות שבמכרז, מערך ההזדהות תוגדר מדיניות סיסמאות שתכלול את הפרמטרים הבאים לכל הפחות:
 - 14.7.1. חוזק הסיסמה - לפחות 10 תווים בשילוב של ספרות ואותיות
 - 14.7.2. מספר ניסיונות שגויים לנעילה - 5 ניסיונות
 - 14.7.3. שמירת היסטורית סיסמאות - עד 5 סיסמאות אחורה
 - 14.7.4. תדירות החלפת הסיסמה - אחת ל-3 חודשים
- 14.8. הספק מתחייב לנתק משתמש שהזדהה למערכת מידע לאחר פרק זמן של 10 דקות ללא פעילות.

15. אבטחת רכיבי תקשורת

- 15.1. הספק מתחייב כי מערכות ומאגרי המידע של המשרד לא יחוברו לסביבת האינטרנט, אלא אם כן קיבל את אישור המשרד לכך מראש ובכתב.
- 15.2. 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 הבקורות והאמצעים הנותנים מענה לדרישה.



אגף טכנולוגיות דיגיטליות ומידע

- 15.3. הספק מתחייב שהעברת המידע בתוך רשת התקשורת, ברשת ציבורית או על גבי רשת האינטרנט תיעשה תוך שימוש בשיטות הצפנה מקובלות בפרוטוקולים מתקדמים.
- 15.4. על ציוד הקצה המשמש להעברת תקשורת (מתגים, נתבים, FW) לעבור הקשחות בהתאם למדיניות היצרן ולעבור עדכוני קושחה.

16. אבטחת עמדות הקצה

- 16.1. חל איסור מוחלט לשמור מידע רגיש בתחנה מרוחקת של המשתמש שלא הותאמה למדיניות מסמך זה.
- 16.2. 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).
- 16.3. הספק מתחייב להתקין רכיב סינון תוכן (Content Filtering) אשר ימנע כניסה של קוד לרשת הספק בעת גלישה לאינטרנט ושימוש בדוא"ל, במידה ויאושר ע"י המשרד.
- 16.4. הספק מתחייב לא לשמור מידע של משרד התחבורה על מחשבים ניידים ו/או טלפונים חכמים.
- 16.5. העברת מידע לרשת המשרד תבוצע לאחר תהליך הלבנה.
- 16.6. הסביבה שתוגדר לצורך טיפול במידע של המשרד תופרד מסביבת העבודה של הספק באמצעות אמצעים לוגיים (FW, סגמנטציה) או ע"י הפרדה פיזית מלאה.
- 16.7. דוחות אירועי מערכת של תחנות העבודה יועברו למערכות הניטור של הספק.

17. שימוש בהתקנים ניידים

- 17.1. הספק מתחייב שלא להוציא חלקי מידע להתקנים ניידים למעט גיבוי המידע כפי שנקבע על ידי המשרד.
- 17.2. 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.
- 17.3. במידה ונדרש מהספק לצורך פעילותו לבצע העלאת חלקי מידע לקלטת גיבוי מתחייב הספק לוודא כי אין ערוב של מידע מסיווגים שונים על אותו התקן.

18. גיבוי, שחזור והתאוששות

- 18.1. מידע של המשרד, הנמצא במערכות הספק יגובה בצורה סדירה. על פי המדיניות שיקבע המשרד.
- 18.2. הספק מתחייב לבצע גיבויים מאובטחים של המידע הנצבר אצלו.
- 18.3. הספק מתחייב לאחסן את מדיית הגיבוי באופן שיבטיח את שלמות המידע ויבטיחו את אפשרות שחזור המידע במקרה של אבדן או הרס.
- 18.4. במידה ויש שימוש בספקי צד שלישי לאחסון גיבויים, יש לאשר את הדבר טרם תחילת העבודה אל מול המשרד.
- 18.5. הספק מתחייב לבצע שחזורים מדגמיים של המדיית המגבות על תשתיותיו לצורך בדיקת התאוששות בהתאם לתוכנית העבודה.
- 18.6. לאחר סיום השחזור המדגמי מתחייב הספק למחוק את המידע ששוחזר.
- 18.7. הספק מתחייב כי שחזור יבוצע אך ורק באישור מנהל אבטחת המידע של המשרד.
- 18.8. הספק מתחייב כי במידה ובוצע שחזור יתועדו כל הליכי השחזור כולל זהותו של מבצע השחזור.
- 18.9. הספק מתחייב למנוע עירוב מידע מסיווגים שונים בזמן השחזור.



אגף טכנולוגיות דיגיטליות ומידע

18.10. הספק יערך לרציפות תפקודית ולהתמודדות עם מצבי משבר בסייבר בהתאם לתרחישי האיום שיוגדרו ויעודכנו מעת לעת על-ידי מערך הסייבר הלאומי ומשרד התחבורה. ההיערכות תכלול לכל הפחות גיבוש מדיניות ונהלי תגובה לאירועי סייבר, הגדרת תפקידים אחריות, הכנת תשתיות חלופיות, גיבוי המידע והגדרת חלופות לתהליכים מרכזיים.

19. שרשרת אספקה

- 19.1. הספק יודא כי מוצרים ושירותים התומכים בתהליכים ומערכות חיוניות של המשרד, נוקטים אמצעי אבטחה בהתאם לסטנדרטים מקובלים בתחום ובהתאם להנחיית יה"ב 5.19 "שרשרת אספקה" והנחיית חטיבת אבטחת מידע וסייבר.
- 19.2. **פירמידת הכשרה והסמכה של ספקים** מבוססת על ספקים במשק אשר עברו תהליך סקר סיכונים באמצעות בודק, מוגשים על ידי הבודק לגוף התעדה אשר מורשה להנפיק לספק תעודת "ספק מאושר". לטובת וידוא שמירה על רמת ביקורת נאותה במשק, מערך הסייבר יבצע בקרה על תקינות פעילותם של גופי ההתעדה, להלן "מאגר ספקים מאושרים" – צורת הסמכה **A** וצורת הסמכה **B**.
- 19.3. הספקים ידורגו לפי שתי צורות ההסמכה הנדרשות A/B. **זירוג הספק יתבצע לפי רמת הקריטיות הגבוהה ביותר של אותו ספק, כאשר הציון הסופי (מבין שלוש רמות הסיכון ו-2 צורות ההסמכה A/B) ייגזר מפוטנציאל הנזק המרבי.**
לדוגמה: ספק אשר בקריטריון אחד נמצא בצורת הסמכה A וביתר הקריטריונים נמצא בצורת הסמכה B, יסווג כספק ברמת פוטנציאל נזק A.
- 19.4. לטובת חישוב פוטנציאל הנזק, ניתן לעשות שימוש במספר קריטריונים, כגון אלו המוצגים בטבלה הבאה:



אגף טכנולוגיות דיגיטליות ומידע

דירוג רמת סיכון	*ספקים בצורת הסמכה A (פלטניה)-	*ספקים בצורת הסמכה B (זהב)-
הסבר כללי על כל צורת הסמכה	נדרשו לענות על שאלון הספקים בעזרת בודק ספקים מוסמך יחד עם ביקורת צד ג' המתבצעת ע"י מכון בדיקת תאימות מורשה מטעם מערך הסייבר הלאומי.	מדובר בהצהרה עצמית של ספק, כלומר צורת הסמכה זו כוללת הצהרת מורשה חתימה (לרוב סמנכ"ל/ מנכ"ל הארגון/היועמ"ש) מטעם הספק על עמידתו במתודולוגיית שרשרת האספקה של מערך הסייבר הלאומי. מעבר לאמור, אמנם לא מדובר בחובה, אך <u>המערך ממליץ על בדיקה פנים ארגונית של המתודה בעזרת בודק ספקים מוסמך.</u>
רמת סיכון 1	רמת סיכון זו, לא קיימת בתהליך התעודה ע"י מכון בדיקת תאימות מורשה מטעם מערך הסייבר הלאומי.	רמת הסיכון הבסיסית ביותר שכל ספק נדרש באופן מוחלט ליישם, רמה זו מתאימה לספקים אשר מהווים סיכון דיגיטלי נמוך ללקוח שלהם. (19 בקרות). { ספק אשר לא מחזיק במידע של הארגון ואין לו נגישות למידע או תשתית של הארגון, וכן בספק שמחזיק במידע של הארגון אך פרסום של המידע או שיבוש שלו לא יגרום נזק לארגון.
רמת סיכון 2	לרוב תהיה כאשר הספק מהווה סיכון משמעותי לארגון, כברירת מחדל ארגוני SMB יישמו רמה זו. (מכילה את 19 הבקרות של רמה +1 38 בקרות נוספות לרמה 2 - כלומר 57 בקרות סה"כ). { ספק המחזיק מידע של הארגון או יש לו נגישות למידע או תשתית של הארגון, אשר תקיפתו עלולה להוות נזק מהותי לארגון }.	
רמת סיכון 3	המאובטחת ביותר, ליישום בספקים אשר מהווים סיכון משמעותי ואף קריטי ללקוח, לרוב ייושם בארגונים גדולים. (מכילה את כל הבקרות של הדרישות רוחביות, כלומר את כל רמות הסיכון 1,2,3, מדובר ב-63 בקרות סה"כ). { ספק המחזיק מידע של הארגון או יש לו נגישות למידע או תשתית של הארגון, אשר תקיפתו עלולה להוות נזק מהותי לארגון }	

- 19.4.1. ספקים שדורגו ברמה A (פלטניה) - יידרשו להוכיח את רמת ההגנה שלהם בדרישות שאלון הספקים המופיע במערכת יוב"ל באמצעות בודק ספקים/גורם בדיקה מוסמך. ספק A, שהוגדר כספק מהותי/קריטי ברמת הסמכה "הערכת צד שלישי/יועץ" ידרשו לפנות למאגר בודקי ספקים - ספקים אלו לא ימלאו את השאלון באופן עצמאי אלא ע"י הבודק (לצפייה ברשימת הבודקים המוסמכים בקישור הבא).
- 19.4.2. ספקים שדורגו ברמה B (זהב) - יידרשו לענות על השאלון הספקים ויחתימו עורך דין או את מנכ"ל המשרד על הצהרת הספק לגבי רמת עמידתו בדרישות ההגנה שבשאלון.



אגף טכנולוגיות דיגיטליות ומידע

- 19.5. טרם ההתקשרות, המשרד יגדיר לספק מהי רמת הסיכון שלו על פי הקריטריונים שתוארו ובנוסף יוגדרו לספק מהן פעולות שעליו לבצע לצורך מימוש רמת ההגנה הנדרשת זאת בהתאם להנחיות מערך הסייבר הלאומי, כמפורט באתר <https://www.gov.il/he/departments/news/querysupply> ;
- 19.6. במקרה בו הספק עבר התעדה והינו מוסמך בהתאם להנחיות מערך הסייבר הלאומי כאמור, על הזוכה להציג את תעודת "ספק מאושר" ובנוסף את תוצאות הסקר.
- 19.7. ספק מהותי (ספק שדורג ברמה A) נדרש להציג תעודת "ספק מאושר" מטעם גוף התעדה מורשה. התעודה מונפקת לאחר מבדק שמבוצע ע"י בודק תאימות סייבר מוסמך לשרשרת אספקה ארגונית. המבדק ייערך על-פי שאלון ספקים של מערך הסייבר הלאומי, לכל סוגי ההתקשרויות (דרישות רוחביות, פיתוח תוכנה, אחסון/עיבוד מידע בענן, גישה מרחוק) ולפי רמת הטמעה של ספק בהתקשרות מהותית.
- 19.8. ספקים שהשפעתם על תהליכים קריטיים נמוכה יותר, יידרשו להשיב על שאלון הספקים של מערך הסייבר ברמת הוכחה של הערכה עצמית או הערכה עצמית בצירוף ראיות, בהתאם להערכת הסיכונים של המפעיל.
- 19.9. באחריות הספק למלא את הפרטים הבאים טרם ההתקשרות ולהעבירה לחטיבת אבטחת מידע וסייבר :

מיפוי ספקים				
שם הספק	סוג השירות/מוצר אותו הוא מספק	איש קשר מצד המשרד אל מול הספק	פרטי התקשרות מול נציג הספק לשאלות בנושא סייבר	סוג השירות הניתן (שירות מבוסס ענן/פיתוח תוכנה/גישה מרחוק/דרישות רוחביות)

- 19.10. אחת לשנה יבוצע תיקוף של רמת ההגנה של הספק באמצעות מענה על שאלון הספקים בהערכה עצמית.

20. פיקוח וביקורות תקופתיות

- 20.1. 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.
- 20.2. 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:
- 20.2.1. בקרה על תהליכי ונהלי עבודה רלוונטיים לעבודת הספק מול המשרד ;
 - 20.2.2. יישום אמצעי אבטחת המשאב האנושי בחצרות הספק ;
 - 20.2.3. יישום אמצעי אבטחה פיזית וסביבתית בחצרות הספק ;
 - 20.2.4. יישום אמצעי אבטחה לוגית בחצרות הספק (כולל כניסה למערכות הספק ו/או בדיקה באמצעות כלים ממוכנים ברשת ומערכות הספק) ;
 - 20.2.5. 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).



אגף טכנולוגיות דיגיטליות ומידע

21. סיום התקשרות

- 21.1. 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).
- 21.2. 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 [בקישור 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'.



אגף טכנולוגיות דיגיטליות ומידע

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.