אל: המציעים שנרשמו להשתתפות במכרז

ל' בתשרי, תשפ"ג
25/10/2022

נספח – פרק הגנת סייבר ואבטחת מידע למכרז סביבת עבודה דיגיטלית

1. **כללי**

1.1. מערכות המידע מהוות את התשתית התפעולית של משרד החוץ והן חיוניות לפעולתו התקינה של המשרד. פגיעה בהן עלולה לגרום לשיבוש או אף להפסקת מתן שירות ללקוחות המשרד. לפי הגדרה זו, מערכות המידע טעונות הגנה להבטחת ואבטחת הסודיות, השלמות, האמינות, השרידות וההמשכיות התפעולית.

1.2. מערכות המידע של משרד החוץ כוללות מידע רגיש בדרגות שונות של רגישות או חסיון, כאשר הסיווג הכולל הוא רגיש/חסוי מסחרית (מקביל לרמת סווג הביטחון "שמור"), לרבות מידע הטעון הגנה לפי חוק הגנה על הפרטיות ותקנותיו ומידע מסווג בטחונית. מערכות המידע חיוניות לפעילותו התקינה של המשרד ופגיעה בהן עלולה לגרום לשיבוש, תקלות והפסקת מתן השרות.

1.3. במשרד קיימות מערכות מסווגות נוספות שעליהן חלות הוראות החוק וההנחיות של מערך הסייבר הלאומי. הנחיות נוספות יימסרו לספק במידה והוא יידרש לעבודה במערכות אלו.

1.4. משרד החוץ הגדיר את נושא הגנת הסייבר ואבטחת המידע ושמירה על מערך המחשוב כנושא אסטרטגי ובעל חשיבות עליונה, ולפי כך כל ספק הנותן שירותים בנושא המחשוב חייב לעמוד בדרישות המוגדרות בפרק זה.

1.5. לפיכך האמור בפרק זה הינו תנאי מחייב לביצוע העבודה, והפרתו מהווה הפרה יסודית של תנאי המכרז.

2. **רקע**

2.1. הפעילות השוטפת של משרד החוץ מערבת ספקים חיצונים, המספקים לו שירותים שונים. במסגרת השירותים ספקים אלה עשויים להיחשף למידע של משרד החוץ, ליצור מידע עבור משרד החוץ ולשמור עותקים שלו אצלם, לספק תשתיות ועיבוד המידע או לקבל גישה לרשת משרד החוץ ולמידע שלו.

2.2. חלק ממדעי המשרד מסווגים כמידע עסקי, ביטחוני או אישי רגיש, ודליפתם לגורמים בלתי מורשים עלולה לגרום לסיכון ביטחוני או לנזק עסקי/כלכלי, תדמיתי או משפטי משמעותי למשרד ולמדינת ישראל.

2.3. עבור כל ספק, משרד החוץ יגדיר מהם נכסי המידע הרגישים המעורבים במתן השירותים. על-מנת למזער את הסיכונים לפגיעה בסודיות, באמינות ובזמינות המידע, נדרש להגן על המיידעים הרגישים, הן כאשר הם ברשת המשרד והן כאשר הם נמצאים אצל הספקים או באחריותם .מסמך זה יפרט את הנחיות ודרישות אבטחת מידע והגנת הסייבר לספקים בין

שהם יוצרים, מעבדים ו/או מחזיקים מידע רגיש של המשרד בתשתיות המחשוב שלהם או ברשת המשרד.

3. **<u>הגדרות</u>**

המזמין	משרד החוץ
הגנת הסייבר	צוות הגנת הסייבר של משרד החוץ
אתר המזמין	מטה ונציגויות משרד החוץ או כל אתר בו נדרש לתת שירות עבור משרד החוץ בהתאם להנחיותיו
מידע	כל מידע (Information), ידע (Know-How), ידיעה, מסמך, תכתובת, תוכנית, נתון, מודל, חוות דעת, מסקנה וכל דבר אחר כיוצ"ב הקשור באספקת השירותים בין בכתב ובין 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 והכל למעט מידע שהוא נחלת הכלל.
עובדים	כלל הגורמים המועסקים ע"י הספק לצורך מתן השירותים לרבות קבלני משנה ו/או מי מטעמו.
ספק	הספק עמו התקשר המשרד לביצוע השירותים.
הפרויקט/ השירותים	כלל השירותים הנדרשים במסגרת המכרז / הסכם ההתקשרות.
רשת המזמין	רשתות מערכות המידע המשמשות ובבעלות את המזמין.

4. **<u>חוקים ותקנים תקפים</u>**

4.1. בנוסף על האמור בפרק זה על הספק לעמוד ב:

4.1.1. התקנים התקפים לאבטחת מערכות מידע של מכון התקנים הישראלי החלים על המשרד.

4.1.2. דרישות החוק והתקנות להגנה על הפרטיות.

4.1.3. דרישות החוק התקפות לסוג המידע נשוא מכרז זה.

4.1.4. דרישות רגולטוריות התקפות לסוג המידע נשוא מכרז זה.

4.1.5. דרישות מערך ההגנה בסייבר הלאומי. – במידה ויידרש על-ידי מערך סייבר חירום וביטחון.

5. **<u>אחריות</u>**

5.1. הספק ימנה נציג מטעמו (להלן: "נאמן אבטחת המידע"), שירכז את כל פעילויות הספק בהיבט אבטחת המידע ויישא באחריות, בכל הנוגע לקיום הוראות פרק זה (על נאמן אבטחת מידע להיות בקיא בתחום הגנת הסייבר).

5.2. מנכ"ל החברה יחתום על "נספח – כתב מינוי נאמן אבטחת מידע והגדרות תפקיד וסמכויות".

5.3. קורות חיים של נאמן אבטחת המידע יצורופו ב: "נספח – קורות חיים של נאמן אבטחת מידע"

5.4. עד אישורו של המועמד לתפקיד נאמן אבטחת מידע על- ידי הגנת הסייבר מטעם משרד החוץ, יחשב מנכ"ל הספק כנאמן אבטחת המידע .

5.5. לחטיבת הסייבר במשרד ו/או עורך המכרז שמורה הזכות להתנגד לבחירתו של המועמד, וכן תעמוד בפניו הזכות לדרוש החלפתו בכל עת. על הספק למלא אחר ההוראה זו בתוך 10 ימים.

5.6. בעת החלפת נאמן אבטחת מידע מכל סיבה שהיא יש לעמוד בסעיפים 5.2 וסעיף 5.3

6. **<u>נאמן אבטחת המידע</u>**

6.1. נאמן אבטחת המידע ישמש איש הקשר לתחום סייבר מטעם הספק במהלך כל תקופת ההתקשרות וירכז את ביצוע כל הפעולות, הנדרשות מהספק בהוראות נספח זה, מול חטיבת הסייבר במשרד בכל הקשור לנושאי אבטחת המידע.

6.2. נאמן אבטחת מידע יהיה בעל הכשרה מתאימה והחברה תדאג להכשירו לתפקיד הנדרש.

6.3. הספק יעניק לנאמן אבטחת המידע סמכויות, כלים ואמצעים הנדרשים לביצוע תפקידו, לרבות סמכויות אכיפה על עובדי החברה בתחומי אבטחת מידע, וסמכויות המוענקות למבקר פנים. הספק יחתום על טופס נאמן אבטחת מידע הגדרות תפקיד וסמכיות.

6.4. נאמן אבטחת המידע יקבל תדרוך מפורט מנציג חטיבת הסייבר (להלן תחום סייבר), לא יאוחר משבוע ימים ממועד מינויו. התדריך יכלול הסברים והבהרות להוראות פרק זה; בנוסף, ימסרו לנאמן אבטחת המידע דרישות ונהלים כלליים נוספים במידה ויידרש, החלים על כל הגורמים המבצעים פעילויות הקשורות למערך המחשוב במשרד, אשר על פיהם יידרש לפעול, ואותם יידרש להנחיל לעובדי הספק וכל מי מטעמו, הנאמן יחתום על אישור כי קיבל תדריך מתאים, ורק אז יוכל להתחיל לעבוד.

6.5. על נאמן אבטחת המידע להיות בקיא בפרטי נספח זה ובשאר נהלי אבטחת המידע הרלוונטיים, החלים על הספק וכל מי מטעמו, ולאכוף אותם.

6.6. נאמן אבטחת המידע יקיים קשר שוטף עם חטיבת הסייבר ונציג מוסמך של אגף תקשוב, בכל עת שיידרש לכך.

6.7. נאמן אבטחת המידע יתדרך ויעדכן את עובדי הספק בהוראות ובנהלים התקפים ואלה שיינתנו מפעם לפעם.

7. **<u>מהימנות צוות הספק</u>**

7.1. נציגים בצוות הספק שידרשו לעבוד בחצרות הספק יידרשו לעבור בדיקה ביטחונית על ידי קב"ט המשרד, כאשר בדיקה זו מהווה תנאי לתחילת העבודה של כל נציג.

7.2. הספק מתחייב לעדכן את הרשימה בכל עת שיחולו בה שינויים, באחריות הספק לעדכן את חטיבת הסייבר על שינויים ברשימה באופן מידי.

7.3. באחריות נציג הספק לוודא את מילוי הטפסים בעבור כלל העובדים שייקחו חלק בפרויקט מטעמו לרבות קבלני משנה, ולהעבירם לחטיבת הסייבר. הספק יקיים מעקב על אישור הנציגים המאושרים לעבודה.

7.4. הספק יעסיק בכל העבודות הקשורות בביצוע המכרז אך ורק עובדים שאושרו להעסקה על ידי קב"ט המשרד ולא יעסיק במתן השירותים הנדרשים עובדים מטעמו שטרם אושרו, לא יחשוף בפניהם כל חומר הקשור לביצוע הסכם זה בטרם קבלת האישור כאמור.

7.5. הספק לא יאפשר גישה לאתרים בהם יעבוד, לגורמים שאינם מוסמכים לכך, לפי הגדרות המשרד.

7.6. קב"ט המשרד שומר לעצמו את הזכות לפסול כל אחד מהעובדים עפ"י שיקול דעתו ללא צורך בנימוק או הסבר כלשהו והחלטתו תהיה סופית ומכרעת.

7.7. הספק מתחייב לעמוד בלוח הזמנים לביצוע חלקו בפרויקט, ללא תלות באישור ביטחוני לעובדים מסוימים, או בהרחקת עובדים, לפני או במהלך העבודה. ובתנאי שאישור/ סירוב יינתן ע"י קב"ט המשרד תוך 7 ימים ממועד קבלת המסמכים הרלוונטיים מהספק.

7.8. קבלת הכשר ביטחוני עבור עובד הינה עבור הפרויקט שעבורו קיבל את ההכשר ולא מהווה אישור אוטומטי לשיתופו בפרויקטים אחרים.

8. **<u>כרטיס חכם</u>**

8.1. ההזדהות למערכות המזמין הינה באמצעות כרטיס באמצעות כרטיס חכם שהינו כרטיס אישי.

8.2. חל איסור חמור למסור את הכרטיס החכם האישי ואת הסיסמא לעובד אחר כולל הממונים של העובד.

8.3. העברתו של הכרטיס החכם לשימושו של אדם אחר מהווה עברה לחוק המחשבים תשנ"ה (1995) ומהווה עברה פלילית ומנהלתית.

8.4. העברתו של כרטיס החכם לשימושו של אדם הדבר יכול להביא להפסקת עבודתו של העובד ואף להפסקת ההתקשרות של המזמין עם הספק.

8.5. באחריות העובד לשמור על הכרטיס החכם בצורה מאובטחת ולמנוע את אובדנו, גניבתו או השחתתו.

8.6. על העובד לשאת את הכרטיס החכם בכל עת ואסור להשאיר את הכרטיס החכם בקורא הכרטיסים כאשר העובד אינו ליד המחשב.

8.7. חל איסור להפקיד את הכרטיס החכם כתעודה מזהה בכניסה לכל בניין בין אם הוא ממשלתי או אזרחי.

8.8. באחריות העובד לדווח מידית על אובדן/גניבה/השחתה של הכרטיס החכם לחטיבת הסייבר של המשרד

8.9. במקרה של אובדן, גניבה או גרימת נזק כלשהו לכרטיס החכם ישא הספק בעלות הפקת כרטיס חכם חדש והמשרד יקזז את העלות מהתשלום המגיע לעובד או לחברה, בכפוף

לשיקול דעתו של המשרד בלבד. האמור לעיל לא יחול במקרה של שחיקה טבעית של הכרטיס החכם, אשר נובע מעבודה סדירה.

8.10. בסיום המכרז/פרויקט עם משרד החוץ יש להחזיר את הכרטיס החכם לקב"ט המשרד או לנציג חטיבת הסייבר באופן אישי בלבד.

9. **<u>סודיות</u>**

9.1. הספק מצהיר בזאת שידוע לו כי המידע שיתקבל במהלך מתן השירותים עבור משרד החוץ הן במסגרת מכרז זה ו/או מידע נוסף שייחשף אליו תוך ביצוע המכרז הינו בעל רגישות מיוחדת, ואין להעבירו לכל גורם שהוא אשר לא אושר על חטיבת הסייבר ועורך המכרז/המזמין.

9.2. הספק מצהיר שידוע לו כי המידע שיתקבל אצלו ואצל עובדיו או מי מטעמו במהלך מתן השירותים הינו בגדר סודות מקצועיים.

9.3. הספק מצהיר שידוע לו כי העברת המידע האמור עלולה להסב למזמין נזקים משמעותיים במישורים שונים.

9.4. הספק מתחייב לשמור את המידע ו/או הסודות המקצועיים בסודיות מוחלטת ולא לעשות בהם כל שימוש. למען הסר ספק, ומבלי לפגוע בכלליות האמור לעיל, הספק מתחייב לא לפרסם, להעביר, להודיע, למסור או להביא לידיעת כל אדם את המידע ו/או הסודות המקצועיים.

9.5. הספק לא יעביר לכל גורם אחר שבו או עימו הוא קשור שלא לצורך מתן השירותים, כל מידע שהוא הנוגע לשירותים, במהלך תקופת ההסכם ולאחריה, אלא אם כן ניתן לכך אישורו המוקדם של חטיבת הסייבר ובתנאים כפי שייקבעו על ידיו.

9.6. הספק מתחייב לפעול על פי הוראות עורך המכרז והמזמין בכל הקשור לשמירת הסודיות, ובכלל זה להסדרת אבטחת המידע ונוהלי הגישה למידע, לאיסוף, לסימון, לאימות ולעיבוד הנתונים; הספק מצהיר, כי הוא מכיר את הוראות חוק הגנת הפרטיות, התשמ"א-1981, והתקנות שהותקנו על פיו, וכי יפעל כמתחייב מחוק זה ומכל חיקוק אחר הנוגע לשמירתו וסודיותו של המידע שימצא ברשותו.

9.7. כל העבודות הכרוכות במתן השירותים ובביצוע התחייבויות הספק לפי הסכם זה, יבוצעו על ידי עובדים ו/או קבלני משנה אשר הוחתמו על הצהרות סודיות מתאימות בהתאם להוראות הביטחון, כמפורט לעיל ולהלן; על אף האמור לעיל, עורך המכרז יהיה רשאי להפסיק את עבודתו של כל עובד, אם ראה זאת כנחוץ מטעמי בטחון ומכל טעם אחר, לפי שיקול דעתו הבלעדי, ומבלי שיהיה חייב לנמק את החלטתו; הפסקת עבודתו של עובד כאמור לא תשמש עילה לספק לתביעת תשלום או פיצוי כלשהו.

9.8. הספק מתחייב להחתים כל אחד מעובדיו על הצהרת הסודיות בנוסח המופיע כנספח 6 למסמכי המכרז. כמו כן, ככל שהספק יקלוט עובדים חדשים במהלך ביצוע השירותים ולאחר קבלת אישור מקב"ט המשרד להכנסתם לפרויקט, יחתימם על התחייבות כאמור וימציאה למזמין

9.9. העתק הצהרות הסודיות האמורות יועבר לעורך המרכז, במסגרת המכרז.

9.10. הספק מתחייב כי במידה וחלק מהשירותים יינתנו באמצעות ספק משנה, ידאג הספק לכך כי ספק המשנה יעמוד באותן התחייבויות לסודיות בהן התחייב הספק לעמוד. לא יורשה לפעול ספק משנה שלא יעמוד בהתחייבויות האמורות.

9.11. הספק מתחייב לנקוט באמצעי בטחון לשמירת סודיות המידע, כמפורט בסעיף זה.

9.12. הספק ישפה את עורך המרכז בגין כל תביעה כלפיו, או תשלום שישלם בשל גילוי מידע או שימוש במידע, שנגרם בשל הפרת סעיף זה על ידי הספק.

9.13. הספק מצהיר כי ידוע לו שאי מילוי התחייבויותיו על פי סעיף זה מהוות עבירה לפי פרק ז' (ביטחון המדינה, יחסי חוץ וסודות רשמיים) לחוק העונשין, תשל"ז - 1977.

9.14. הוראות והנחיות בנושא שמירה על סודיות ואבטחת מידע יכול ויימסרו על ידי הגנת הסייבר של עורך המכרז בכתב או בעל פה, ויחייבו את הספק ללא יכולת ערעור וללא קבלת תמורה נוספת.

9.15. אם תחול על הספק או מי מטעמו חובה על פי דין לגלות מידע שהוא חייב שמירתו בסוד לפי ההסכם, הוא יודיע על כך לעורך המכרז/ למזמין מראש ובאופן מיידי, כך שעורך המכרז/ המזמין יוכל להפנות לערכאה המתאימה בקשה לצו חיסיון וצו מניעה לשימוש במידע. אם לא יינתן צו כאמור, או אם עורך המכרז/ המזמין יוותר על זכויותיו לגבי מידע מסוים, יהיה רשאי הספק לגלות את אותו חלק מהמידע הדרוש על פי דין ויעשה כל שביכולתו על מנת שהמידע הנמסר יישמר בסוד.

9.16. מוסכם ומוצהר כי ההתחייבויות ההדדיות שבסעיף זה אינן מוגבלות בזמן, ואף יעמדו בתוקפן במקרה של ביטול חוזה זה.

9.17. הוראות סעיף 6 על תת סעיפיו הן הוראות יסודיות בהסכם, והפרתן על ידי הספק תחשב כהפרה יסודית של ההסכם.

9.18. מידע הנוגע לפרויקט לא ייחשף לשום גורם מחוץ למשרדי המזמין ללא אישור בכתב מקב"ט המשרד.

10. **<u>אבטחת מידע ושמירה על המידע – מידע שאינו מסווג</u>**

10.1. הספק לא יחבר מחשבים וכל ציוד אחר לרשת המשרד.

10.2. הכנסת מידע מאמצעי אחסון מגנטיים או אופטיים טעונה אישור כתוב מראש מחטיבת הסייבר.

10.3. לא יבוצע כל ניסיון, לעקוף מערכות הגנה, מגבלות גישה או ניצול פרצות, שלא במסגרת החוקית של ההתקשרות.

11. **<u>שרשרת האספקה</u>**

11.1. בהתאם להנחיות הגופים המנחים באחריות המשרד, טרם ההתקשרות, על הספק לעמוד בהנחיית שרשרת האספקה של מערך הסייבר הלאומי ולהציג אישור לעמידה בהנחיות ע"י מערך הסייבר הלאומי.

12. **<u>עיבוד מידע</u>**

12.1. עיבוד נתונים, מסמכים, תרשימים וכל מידע אחר ייעשה בסביבת העבודה של המזמין בלבד.

12.2. הספק לא יעביר מידע מרשת המשרד אל רשת חיצונית למשרד בכל אמצעי אלקטרוני או אופטי אלא אם כן קיבל אישור בכתב מהגנת הסייבר, ואז העברת המידע תעשה לצורכי עבודה בלבד, ייערך רישום פרטי של המידע המועבר. הספק יפעל לפי הנחיות אבטחת מידע לעיבוד מידע אצל הספק.

12.3. ביצוע שינויים כלשהם במערכות המחשוב והתקשורת של המשרד, שימוש בתוכנות אבטחה חיצוניות והתקנת אמצעי אבטחה חדשים, טעונים אישור מראש ובכתב של מנהל אגף תקשוב והממונה על הגנת הסייבר, לפי הצעה בכתב של הספק ודיון, לפי הצורך.

13. **<u>דרישות הגנת סייבר ואבטחת מידע למערכות המידע של הספק</u>**

ספק שקיבל את אישור חטיבת הסייבר לעבד מידע של המשרד המערכות המידע של המשרד מתחייב לעמוד בדרישות הבאות:

13.1. זיהוי משתמש ברמת MFA או כמינימום שם משתמש וסיסמה.

13.2. מידור הרשאות ברמת מערכת ההפעלה המאפשר למשתמש המורשה בלבד גישה למידע.

13.3. אמצעי הגנה מפני קוד מפגע המתעדכן תדיר.

13.4. הגנת Firewall בין מחשב המשתמש לרשת האינטרנט.

13.5. יכולת תיעוד, ניטור ובקרה (Audit Policy) הגנתיים.

13.6. הספק ומי מטעמו מתחייב בזה כי ישמור בסודיות מלאה ומוחלטת כל מסמך, מידע, פרטים ונתונים מכל סוג שהוא, לרבות נתונים או סודות מסחריים על אודות המזמין (להלן המידע) שיגיעו לידיעתו במישרין או בעקיפין או יופקו על ידו עקב מתן השירותים על פי המכרז.

13.7. הספק יעביר למזמין, לפי בקשתו , את פירוט האמצעים שינקוט כאמור לעיל. הספק מתחייב להשמיד את כל הדוחות, הרישומים, המסמכים ונתוני הביניים שנוצרו במהלך מתן השירותים מיד עם גמר מתן השירותים ולמסור למזמין יחד עם המקור את כל ההעתקים של הדוחות והרישומים הסופיים שהופקו לשם מתן השירותים.

13.8. התחייבויות הספק על פי סעיף זה אינן מוגבלות בזמן, הן תנאי מחייב בתנאי מכרז זה והן מחייבות את הספק ומי מטעמו המעורב בפרויקט.

13.9. בשעות העבודה יהיה המידע בהשגחתו של נותן השירותים המוסמך לראותו או לעסוק בו. השגחה הינה פיקוח פיזי רצוף וישיר.

13.10. כל המידע הנאסף, תוצרי הביניים והתוצרים הסופיים יגובו באופן סדיר על מנת למנוע את אובדנם. הגיבויים יישמרו במקום נפרד מהמקור תוך שמירה על רמת אבטחה שהוגדרה במקור עבור אותו חומר.

13.11. הדפסה, אחסון ומשלוח של החומרים שבידי הספק יהיו על פי הנחיות המזמין.

14. **<u>הגנת סייבר ואבטחת מידע בתחום הספק</u>**

14.1. בקרת כניסה למבנים

14.1.1. החברה תפעיל שמירה ובקרת כניסה למבנים, בהם מותקנות מערכות ומאגרי מידע המשמשים את החוץ.

14.1.2. החברה תקיים שמירה ובקרת כניסה לכל אזור שבאחריותה, ממנו מתאפשרת גישה לתשתיות המקושרות למערכות המשמשות את משרד החוץ.

14.1.3. בקרות הכניסה ונהלי השמירה יוסכמו ע"י קב"ט משרד החוץ טרם מימוש ההתקשרות.

14.2. מסמכים ומצעי מידע

14.2.1. הנחיות על שיטות אבטחת מסמכים וחומר אחר יינתנו על ידי קב"ט המשרד. הספק יהיה אחראי לקבל הנחיות קב"ט המשרד וליישמם בפועל.

14.2.2. הספק יגרוס חומר כתוב שאינו בשימוש ושאינו נדרש יותר המכילים מידע השייך למשרד או החושף מידע, שלא הותר לפרסום ע"י חטיבת הסייבר.

14.2.3. מצעי זיכרון תקולים לא יוחזרו לספק החומרה גם אם הם באחריות במידה והוגדרו כרגישים או מכילים מידע אשר מונעת את החלפתו על ידי ספק החומרה, מצעים אלו יועברו לחטיבת הסייבר להשמדה.

14.3. אישור לעבודה במערכות המידע של הספק

14.3.1. ספק אשר עושה שימוש בענן מכל סוג שהוא לא יוכל לעבד מידע של המשרד במערכותיו וכל המידע יעובד ברשת המשרד.

14.3.2. ספק יעבוד במערכות מידע שלו רק לאחר קבלת אישור פרטני על ידי חטיבת הסייבר ויחתום על הצהרה כי אינו מעבד מידע בענן מכל סוג שהוא.

14.3.3. במקרה וימצא כי הספק עובד בענן למרות הצהרתו, הפרה זו תחשב הפרה יסודית של תנאי המכרז.

14.4. מערכות מידע של הספק

14.4.1. כל המידע הנוגע למשרד החוץ, בין אם גרפי (תרשימים, דיאגרמות, סרטוטים) ובין אם טקסטואלי (תכתובות, נהלים) יישמר על מחשב ייעודי.

14.4.2. המחשב יהיה ללא קישור לאינטרנט מאחורי חומת אש (פיירוול)

14.4.3. המחשב יעבור לפחות אחת לשבוע סריקה מלאה עם תוכנת אנטי וירוס מעודכנת.

14.4.4. המחשב יהיה מוגן בבקרת גישה בשם משתמש וסיסמה. גישה תינתן רק למספר עובדים מוגבל ומורשים על ידי חטיבת הסייבר רק לפי צורך.

14.4.5. החברה תנהל רשימה מעודכנת של כל מורשיי הגישה, לרבות תפקידם ופירוט הרשאותיהם.

14.4.6. בכפוף לדרישות המזמין, החדר בו נמצא המחשב יהיה נעול כשלא עובדים בו והגישה לחדר תהיה מוגבלת לעובדים הספציפיים הזקוקים לו לצורך עבודתם. החדר והמחשב ייבדקו ע"י קב"ט המשרד לפני תחילת הפרויקט ובמהלכו בתאום עם הספק ולאחר מתן התראה מראש.

14.4.7. הספק מתחייב להתקין ולהפעיל מערכות תכנה לבקרה לאבטחת-מידע מתקדמות.

14.4.8. הספק מתחייב להפעיל פונקציות אבטחה במערכות הפעלה בכל המערכות נשוא ההתקשרות.

14.4.9. הספק מתחייב להפעיל מנגנוני בקרת תקשורת ממערכות אחרות (המקושרות לחברה) ועלולות להשפיע על רמת אבטחתן של המערכות המשמשות את משרד החוץ במישרין או בעקיפין.

14.4.10. סוגי מערכות האבטחה ופונקציות האבטחה הנדרשות יסוכמו טרם מימוש ההתקשרות.

14.4.11. החברה מתחייבת להוסיף מערכות הגנה ובקרה, אשר תידרשנה ע"י משרד החוץ במסגרת אחריות מנהל המאגר, כמתחייב מהחוק ופרשנותו המקצועית או במסגרת הצורך בשיפור מערך האבטחה.

14.5. הגנת סייבר ואבטחת מידע בתקשורת

14.5.1. החברה מתחייבת לממש הגנה על מערכת התקשורת בהתאם לרמת רגישות המערכות נשוא ההתקשרות.

14.5.2. במידה ויהיה פער בין מערכי אבטחה הנדרשים לקיים בידי החברה, תתחייב החברה להפריד את תשתיות התקשורת, כך שהתקשורת למערכת החוץ תאובטח כנדרש, לחילופין, תירכשנה מערכות אבטחה, כפי שיסוכם על דעת משרד החוץ

14.6. בקרות גישה

14.6.1. הספק מתחייב להשתמש במערכות תוכנה מתקדמות, לשם ניהול בקרות גישה לתשתיות התוכנה, לבסיסי הנתונים ולמאגרי המידע.

14.7. דוחות בקרה

14.7.1. החברה מתחייבת להפעיל ולנהל דו"חות פעילות ודו"חות בקרת כשלים וחריגות בשרתים ובעמדות הקצה, בתשתיות תקשורת, בתשתיות תכנה ובבסיסי נתונים - נשוא ההתקשרות.

14.7.2. החברה מתחייבת להעביר למשרד החוץ לפי דרישה או בהליך שוטף – דו"חות בקרה, שידרשו בתוספת – ב' או באופן יזום ע"י משרד החוץ .

14.7.3. החברה מתחייבת כי הדו"חות יועברו למשרד כשהם ממוינים על-פי הנתונים, שידרשו מהחברה.

14.7.4. דו"חות, שידרשו מהחברה לאחר סגירת ההסכם ותחילת מימוש ההתקשרות, ואשר נדרש עבורם פתוח או רכש מערכות, תקבע השתתפות משרד החוץ במימון (כמפורט בסעיף - מימון).

14.8. גיבוי

14.8.1. החברה מתחייבת לספק מערכי גיבוי, שרידות והתאוששות ברמות גיבוי שונות :

14.8.1.1. גיבוי שוטף של מאגרי מידע ועדכוני תוכנה.

14.8.1.2. גיבוי דוחות בקרה לתקופה של שנה לפחות מיום רישום הדו"ח .

14.9. מחויבות לדיווח מיידי ולשיתוף פעולה באירועי אבטחה בחקירת אירועים או חשדות, לחריגות אבטחה.

14.9.1. בכל מקרה של אירוע סייבר/ חשד לאירוע אצל הספק

14.9.2. בכל מקרה של תקלת אבטחת מידע בתחומי המתחם ו\או המחשבים המשמשים לפרויקט משרד החוץ

14.9.3. בכל אירוע בו מעורב גורם-חוץ או אחד מעובדיו, או שקיים חשד למעורבות שיש עמה השלכה ישירה או עקיפה על ביטחון משרד החוץ או בטחון ענייניו.

14.9.4. בכל הפרה או חשד להפרה של חוקים, תקנות או נהלי אבטחת-מידע.

15. **<u>שימוש בענן</u>**

15.1. בהתאמה לנספח מתן שירותים בענן.

16. **<u>אחסון המערכת</u>**

16.1. מערכת המאוכסנת ברשת המשרד:

16.1.1. הרשאות הגישה לרכיבים השונים של המערכת אשר יתבצעו באמצעות הרשת המשרדית של המזמין יבוצעו ע"י אגף תקשוב. הספק ומי מטעמו יהיו כפופים לתנאי הביטחון הקיימים באתרי המשרד והנחיות לפני תחילת העבודה ובמהלכה.

17. **<u>מערכת מחשב ומידע</u>**

17.1. ארכיטקטורה - הספק יציג לאישור את הארכיטקטורה המוצעת הרלוונטית (לא ארכיטקטורה כללית) לאישור חטיבת הסייבר לפני תחילת העבודה והתקנת המערכת.

17.2. חומרה - הספק יציג רשימה של הציוד אותו הוא מתכוון להתקין לפני תחילת העבודה. הרשימה תכלול: שם הרכיב + FQDN, יעוד הרכיב, כתובות IP, יצרן, דגם, מספר סריאלי , תוכנת הפעלה + גרסה.

17.3. הקשחה - הספק יציג רשימות תיוג להקשחה לכל פריט בנפרד (לאחר ביצוע) אותן יגיש עם אספקת הציוד. במידת הצורך, יקבל הספק רשימת תיוג ספציפית למכשיר אחד או יותר ויגיש אותה לאחר המילוי עם הציוד.

17.4. מערכות הפעלה ותוכנה - באחריות הספק לדאוג לעדכן את מערכת ההפעלה ותוכנות מסחריות אשר נעשה בהן שימוש במסגרת המכרז. במקרה של הודעה של הספק התוכנה על עדכון תוכנה קריטי על הספק לעדכן את התוכנה תוך שבוע ימים בתיאום עם חטיבת הסייבר במשרד החוץ.

17.5. מערכות לא נתמכות – על הספק להיערך מראש להחלפת מערכות שהיצרן מסיים את התמיכה בהם.

17.6. הקשחת ציוד - הרכיבים הדורשים הקשחה הם שרתים, מחשבים וציוד תקשורת אקטיבי (נתבים, מתגים). ההקשחה תתבצע אל מול התפקודים הנחוצים של המערכת. הגישה להקשחת הרכיבים תתבסס על שני עקרונות. נטרול שירותים, הרשאות ותפקידים לא נחוצים. מזעור אפשרויות גישה ותיעוד (לוגים) מקסימאלי.

17.7. שדרוג - במידה ותידרש התקנת מערכת הפעלה עדכנית, יש להודיע על כך חודשיים מראש לאגף תקשוב.

17.8. תמיכה תחזוקה מרחוק - התחברות לתחזוקה מרחוק של המערכת תתאפשר רק לאחר אישור לספק לבצע תחזוקה מרחוק במערכת על ידי חטיבת הסייבר. ותבוצע עם עובד המשרד בלבד ובנוכחותו.

17.9. כל העדכונים לתוכנות ולמערכות ההפעלה יתבצעו דרך מעטפת הלבנה בלבד. הספק יביא אתו מדיה המכילה עדכונים ובסיוע אנשי משרד החוץ ילבין את המידע לפני העדכון. למען הסר ספק – אין לחבר מדיות חיצוניות מכל סוג שהוא למערכות המשרד.

18. **<u>פיתוח תוכנה</u>**

18.1. פיתוח התוכנה יבוצע על פי עקרון של פיתוח מאובטח. המערכת תכלול את האפשרות לאיסוף לוגים על מנת לנתח ולבצע תחקור אירועים. במערכת תעשה שימוש בשיטות ובאמצעי ההזדהות הסטנדרטים במשרד.

18.2. הפיתוח והעבודה תתבצע בטכנולוגיה של שלוש סביבות עבודה: סביבת פיתוח (DEV), סביבת ניסוי (TEST) וסביבת הייצור (PROD).

18.3. שלושת הסביבות הנ"ל תפעלנה על גבי שרתים נפרדים. כל סביבה תפעל באופן עצמאי, מנותקת מהסביבות האחרות, כאשר הקישור היחיד בין הסביבות הינו באמצעות firewall.

18.4. כל דרישות האבטחה מתייחסות לכל שלושת הסביבות.

18.5. בסביבות הפיתוח (DEV) וסביבת הניסוי (TEST) אין לכלול נתוני אמת ומידע רגיש.

19. **<u>מאגרי מידע</u>**

19.1. הספק מתחייב לעמוד בחוק הגנת הפרטיות ובכל הנחיות הרשות להגנת הפרטיות במשרד המשפטים, אי קיום הוראה זו מהווה הפרה יסודית של המכרז וההסכם.

19.2. לאשר את אמצעי האבטחה הפיזיים הננקטים להגן על מאגר המידע עם קב"ט המשרד.

20. **<u>זכויות בחומר</u>**

20.1. מוסכם בזאת כי לספק אין ולא תהיינה כל זכויות בחומר שיועבר לידיו על ידי משרד החוץ לצורך ביצוע השירותים לפי הסכם זה, והספק יהיה רשאי לעשות שימוש בחומר כאמור אך ורק במסגרת ולשם ביצוע השירותים ובהתאם לכל יתר הוראות הסכם זה.

20.2. מוסכם בזאת כי המזמין יהיה בעלת כל הזכויות בכל חומר שיתקבל, ייאסף, יוכן ויעובד על ידי הספק במסגרת מתן השירותים לפי הסכם זה, לרבות רישומי הפניות והדיווחים

שהספק מעביר למשרד, המשרד יהיה רשאי לעשות בחומרים כאמור כל שימוש שתמצא לנכון, בכפוף להוראות כל דין.

21. **<u>העברת נתונים</u>**

21.1. אין לאזכר קיומן של רשתות מסווגות ("שמור", "סודי" ו-"סודי-ביותר") או מידע מסווג בהתכתבויות ו/או במסמכים במהלך הפרויקט.

21.2. יש לצמצם ככל האפשר הוצאת מידע ממשרדי המזמין, הוצאת מידע באישור בעל המידע וקב"ט המשרד.

21.3. העברת קבצים תתבצע בדרך שתקבע בעת הבקשה.

22. **<u>סקרי סיכונים</u>**

22.1. אחת ל- 12 חודש מתחייב הספק לבצע סקר סיכונים, באמצעות צד ג' , אשר יוסכם על דעת חטיבת הסייבר של המשרד.

22.2. במקרים מסוימים, בהתאם לרמת הרגישות של המידע הקיים במערכת וכפוף להנחיה של קב"ט המשרד ידרוש מהספק לבצע סקר סיכונים אחת לשמונה עשר חודשים.

22.3. הסקר יקיף את כלל המערכות המשמשות את המזמין, לרבות מערכות של הספק המקושרות על אותה תשתית או פועלות במשותף, או שניתן בדרכים עקיפות להגיע דרכן אל מערכות המזמין וכל ממשקי העבודה הקיימים למערכת .

22.4. ממצאי הסקר ומסקנות הסוקר, יועברו אל חטיבת הסייבר – לכל היותר 30 יום מהגשתן לספק.

23. **<u>אירועי סייבר ואבטחת מידע</u>**

23.1. הספק מתחייב לנהל דו"חות ומעקב איתור אירועים חריגים, דיווח וטיפול בהם.

23.2. הספק, אם יידרש יציג את יומן החריגים לנציגי משרד החוץ, במועד העברת הדרישה.

23.3. על הספק ומי מטעמו לדווח על כל ליקוי אבטחת מידע, שיתגלה במערכות החברה, ישירות למנהל. ליקויים מהותיים הנוגעים בין במישרין ובין בעקיפין למערכות החוץ או למערכות, נשוא ההתקשרות - ידווחו לחטיבת הסייבר של המשרד.

23.4. אירוע אבטחה אשר יתגלה במשרד ע"י עובדי החברה, ידווח לחטיבת הסייבר במשרד במידי.

23.5. אירוע אבטחה אשר יתגלה ע"י צוות הספק, ידווח לחטיבת הסייבר במשרד.

23.6. בידי הגנת הסייבר של משרד החוץ, הסמכות להגדיר ולקבוע מהו אירוע או ליקוי מהותי, אופן הדיווח, הגורמים המדווחים והנמענים לדיווח.

23.7. בסמכות חטיבת הסייבר לשנות מדרישות אבטחת המידע הנדרשות מהספק בעקבות אירוע אבטחת מידע ועל הספק לציית לדרישות.

24. **<u>בקרה ופיקוח אבטחת מידע</u>**

24.1. בסמכות חטיבת הסייבר וקב"ט המשרד ו\או נציג שיוסמך על ידם לבצע סקרי-סיכונים, ביקורות פתע, בדיקות ביטחוניות, בדיקות חסינות, ביקורות הדרכה וכל ביקורת אחרת באתר הספק, אשר מטרתה לבחון תקינות מערכי אבטחה, סיכונים, יעילות פתרונות אבטחה או בדיקת חשדות, אשר להם זיקה או השפעה על אבטחת המערכות המשמשות את המשרד .

24.2. עורך המכרז יהיה רשאי לערוך, על פי שיקול דעתו, או לדרוש מהספק לבצע בדיקות אקראיות לבחינת השירותים שיסופקו לעורך המכרז כמפורט במכרז.

24.3. הספק יאפשר לעורך המכרז או למי שימונה מטעמו לפקח על אספקת השירותים המבוקשים, טיבם ואיכותם, ולהיכנס לצורך זה לכל מקום, על מנת לבדוק ולפקח על אופן מילוי התחייבויותיו.

24.4. הספק מתחייב לשתף פעולה עם נציגי המזמין ועם המפקחים, בכל הנוגע לביצוע הפרוייקט ומילוי כל יתר התחייבויותיו על פי המכרז וההסכם, וימלא אחר כל הנחיה של נציגי המזמין והמפקחים, בכפוף להוראות המכרז וההסכם. בכלל זה, ימסור לנציג המזמין ולמפקחים כל מידע או דיווח שיידרש על ידיהם, במועד ובאופן שייקבע על ידיהם; יאפשר לנציגי המזמין ולמפקחים לבקר במשרדיו ובכל מקום אחר שבו הוא מבצע את התחייבויותיו על פי הסכם זה, לעיין בכל מסמך ולבדוק את הנעשה בהם בקשר לשירותים ולביצוע התחייבויות הספק על פי הסכם זה, ובלבד שכל ביקור כאמור יתואם מראש עם הספק.

24.5. למען הסר ספק, מובהר ומוסכם, כי נציגי המזמין והמפקחים אינם רשאים ואינם מוסמכים לחייב את המזמין בכל חיוב כספי, בין שיש בו כדי לשנות את סכום התמורה על פי הסכם זה ובין שיש בו כדי להטיל עליו חיובים נוספים בקשר להתאמות, שינויים ושיפורים (שו"ש), וחיובו של המזמין בעניינים אלה ייעשה אך ורק במסמך בכתב, חתום על ידי מוסמכי החתימה של המזמין.

24.6. הספק, באמצעות מנהל הפרויקט שימנה, יגיש למזמין דוחות תקופתיים ערוכים באופן ובתדירות שיורו נציגי המזמין או המפקחים.

25. **<u>סיום ההתקשרות</u>**

25.1. על הספק יהיה לשתף פעולה עם נציגי המזמין לצורך העברת מאגר הנתונים, מסמכים, אמצעי אחסון וכל מידע נוסף שיקבל מהמשרד למזמין, או למי שייקבע על ידו, בסיום תקופת ההתקשרות.

25.2. בעת ההעברה המידע שיתקבל ייבדק מול רשימת המצאי. במקרה של פערים בין רשימת המצאי לבין המידע המוחזר או במקרה בו רשימת המצאי חסרה הספק מתחייב לפעול על פי הנחיות חטיבת הסייבר והחלטתו תהיה סופית ומכרעת.

25.3. מנכ"ל הספק יחתום על מסמך המאשר שלא נשאר ברשותו כל מידע ששייך למזמין מתוקף מכרז זה.

25.4. מנכ"ל הספק יחתום על מסמך שבו הוא מודע כי הסכם הסודיות של החברה ועובדיה לרבות ספקי משנה מחייב אותם גם לאחר סיום ההעסקה

נספח – כתב מינוי נאמן הגנת סייבר ואבטחת מידע והגדרות תפקיד וסמכויות

הריני ממנה את מר/גב

מספר זהות	שם משפחה	שם פרטי	המועסק בחברה בתפקיד

כנאמן הגנת סייבר ואבטחת מידע בחברה והריני מקנה לו את תחומי האחריות והסמכויות הבאות:

1. תכנון מדיניות הגנת סייבר אבטחת המידע ובקרה על יישומה.
2. תכנון וביצוע סקרי סייבר ואבטחת מידע, ווידאו כי סקרי אבטחת המידע ומבדקי החדירה נערכים על ידי גורם מקצועי, עצמאי, בלתי תלוי וחיצוני באושר על ידי חטיבת הסייבר.
3. ניהול ההרשאות ודרכי הגישה למשתמשים.
4. תכנון ויישום תכנית התאוששות DRP.
5. ניהול ההגנה על מערכות המידע והתקשורת.
6. אחריות לבדיקה ואישור כניסת ספקים למערכות החברה.
7. אחריות להחתמת עובדים חדשים על נהלי החברה בתחום אבטחת המידע וביצוע תדרוך אבטחת מידע ע,י חטיבת הסייר / קב״ט המשרד בזמן קליטתם למכרז.
8. הגדרת בקרות פיזיות, בהתאם להערכת הסיכונים, ע״י קב״ט המשרד. בקרות אלה יכללו נושאים כגון בקרת גישה, הגנה פיזית של נכסים וכיו״ב.
9. הגדרת מדיניות סיסמאות ותהליכי גישה למערכות מידע והתקשורת.
10. הגדרת דרישות הגיבוי למערכות המידע והתקשורת בחברה בהתאם לצרכים השונים.
11. בקרת איכות הגיבויים ואופן אבטחתם.
12. מתן אישור להעברת מידע בטרם העברת המידע לגוף ציבורי.
13. דיווח לחטיבת הסייבר במשרד החוץ על אירועי אבטחת מידע או על חשד לאירוע אבטחת מידע, וביצוע הנחיות חטיבת הסייבר של משרד החוץ בהמשך לדיווח.
14. בסמכותו של נאמן אבטחת המידע לזמן כל עובד/מנהל בחברה לשימוע בפני ההנהלה, ככל שהעובד/מנהל יחרוג מנהלי אבטחת המידע.
15. בהתאם לשיקול דעתו הבלעדית של נאמן הגנת סייבר ואבטחת המידע, להשעות/לחסום כל משתמש שיחרוג מנהלי הגנת סייבר ואבטחת המידע.

תאריך	מס זהות	שם ומשפחה	תפקיד	חתימה

נספח – קורות חיים של נאמן הגנת סייבר ואבטחת מידע

יש לצרף כאן קורות חיים של נאמן הגנת סייבר ואבטחת מידע.

שד' יצחק רבין 9, ת.ד. 3013, ירושלים 91035 טל'. 02-5303361
Shderot Yitzhak Rabin, P.O.Box 3013, Jerusalem, 91035 Tel:972-2-5303 361

נספח – דרישות פרטניות בהיבטי הגנת סייבר ואבטחת מידע

1. **דרישות טכניות ותהליכיות של המערכת המוצעת:**

1.1. אופן עמידת המוצר ברגולציית הגנת פרטיות.

1.2. מדיניות ניהול זהויות, בקרת גישה (הזדהות) והרשאות {תיאור יכולות בקרת גישה וניהול משתמשים.

1.3. יש לפרט יכולות מניעת דלף מידע ושליטה במידע (יכולות הצפנה, הסתרה, ערבול, האפלה וכדומה) והגנה על המידע במנוחה בתנועה ובעיבוד (in Motion, in Process & at Rest).

1.4. המערכת תתמוך ביכולת המזמין לערפל (Obfuscation) ו/או להתמים/ להסתיר (Anonymization\ Masking) ו/או לערבל ו/או להצפין מידע ביצירתו, שינועו/ עיבודו ואחסונו על-פי יכולת ניהול זהויות, הרשאות ומידור.

1.5. ככל שקיימים ממשקים לתשתיות ארגוניות כגון: ניהול קריאות, שירותי IPTEL מבוססי "שירלי", Active Directory, שרתי Exchange יש לפרט אופן ההגנה המוצע עליהם.

1.6. פירוט אופן ניהול חולשות והקשחות, אפליקטיביות ותשתיתיות.

1.7. לפרט אופן העמידה בהיבטי פיתוח מאובטח (באם מבוסס NIST 800-218 מספקת הצהרה בלבד).

1.8. תיעוד, ניטור ובקרה (Audit Policy) בהיבטי הגנת סייבר ואבטחת מידע, לרבות מתן קישור ממוכן למערכות הניטור האבטחתי המרכזיות של המזמין.

2. **בדיקות הגנת סייבר ואבטחת מידע**

2.1. בדיקות הקבלה של המערכת יכללו בדיקות הגנת סייבר אבטחת מידע באמצעות סקרי סיכונים ממוקדים ולרבות מבדקי חדירה (Penetration Tests).

2.2. במהלך תקופת הבדק תחול על הספק אחריות בלעדית לתיקון/השלמת כל ליקויי הגנת הסייבר ואבטחת המידע שיתגלו, במועד הקצר ביותר האפשרי ובלוח זמנים שיוצג ע"י ספק למזמין ויאושר ע"י מנהל הגנת הסייבר.

2.3. בהנחת הצעה להתקנה במספר סביבות (הפיתוח, הבדיקות והייצור), הן תהיינה זהות בהיבטי יכולות הגנת סייבר ואבטחת המידע, לרבות עמידה בתקני הגנת סייבר ואבטחת מידע מחייבים.

3. **נושאים רוחביים**

1.1 נדרש לספק דוגמאות ל:

1.1.1 מסמך ניתוח סיכונים (Risk Analysis), לרבות מסמך ומדיניות הערכת סיכונים (Risk Assessment) לשירות המוצע.

1.1.2 תמונת מצב של ניתוח פגיעויות (Vulnerability Assessment).

1.2 אופן יישום תכן פרויקטלי – מסמכי תכנון (HLD, LLD וכדומה).

שד' יצחק רבין 9, ת.ד. 3013, ירושלים 91035 טל'. 02-5303361
Shderot Yitzhak Rabin, P.O.Box 3013, Jerusalem, 91035 Tel:972-2-5303 361