

בלמ"ס



**פניה לקבלת הצעות לנותני שירותים  
אנשי אבטחת מידע - מס' 30/2022**

פניה לקבלת הצעות לנותן שירותים - מומחה טכנולוגיות הגנת סייבר -

מס' 30/2022

1. על פי מכרז מממ-1-2009 להספקת שירותי מחשוב למשרדי הממשלה והודעת המכרז המרכזי מ. 16.2.11 מהדורה 22, הנכם מוזמנים בזה להגיש מועמדים למתן שירותים בתחום תומכי יחידות מחשוב, לפי הפרטים הבאים:
  - 1.1 פניה זו הינה תיחור עבור 1 נותן שירותים למשרות בודדות ואינה תיחור צוות.
  - 1.2 אשכול: 6, תפקיד 6.4, רמה ג' (מומחה טכנולוגיות הגנת סייבר).
  - 1.3 תיאור התפקיד הנדרש: איש אבטחת מידע וסייבר בפרופיל העיסוקים שיפורטו בהמשך, אשר יספק שירותים עבור אגף הביטחון במטה הוא"א.
  - 1.4 מספר נותני השירותים המבוקשים: אחד.
- מספר נותני השירותים שנדרש כל ספק להציע לכל תפקיד: ככל שספק יבחר להציע מספר גבוה יותר של מועמדים, יהיה רשאי המשרד, עפ"י שיקול דעתו הבלעדי, שלא לשקול כלל את מועמדותם של נותני השירותים המוצעים מטעמו של הספק ולפסול את הצעתו מטעם זה בלבד. המשרד שומר לעצמו את הזכות לזמן לראיון התאמה אך ורק מועמדים שעמדו בדרישות הסף.
- 1.5 היקף השירותים (כמות שעות בחודש) ותעריף מרבי:
  - א. עבור תפקיד 6.4 רמה ג': כ 30 שעות בחודש-ותעריף מירבי של 400 ₪ לשעה.
- 1.6 ציוד נדרש: לא נדרש.
- 1.7 תקופת העבודה: שנתיים+ 3 אופציות בנות שנה כ"א.
- 1.8 מועד תחילת עבודה משוער: 01/12/2022, בתיאום עם החברה ונותן השירות ניתן להקדים.
- 1.9 מקום מושבו של נותן השירותים: יבנה, עם נסיעות עיתיות לאתרים אחרים של המזמין.
- 1.10 דרישות סף בנושא השכלה: (על פי הקבוע בהודעת מכרז מרכזי מ. 16.2.11 מהדורה 22):

אקדמאי בעל תואר ראשון במקצועות המחשוב ו/או המדעים המדויקים ו/או הנדסה טכנולוגית או הנדסאי בוגר מגמת מחשבים/ טכנולוגיה או חסר תואר כנ"ל, בעל הכשרות מקצועיות בתחום הגנת הסייבר בהיקף משמעותי (400 שעות במצטבר) או בוגר יחידה טכנולוגית בצה"ל (ממר"ם, 8200, תקשוב ויחידות מקבילות) ו/או ברא"ם ובלבד שעסק בתחום הטכנולוגי בכפוף לאישור המתאים או בעל הסמכה למקצוע זה אשר נתקבל מאת מערך הסייבר הלאומי.

## בלמ"ס

### 1.11. דרישות סף נוספות:

1.11.1. ניסיון של 6 שנים לפחות בתחום תכנון, יישום והטמעת מענה תשתיתי טכנולוגי להגנת הסייבר, תוך שילוב תשתיות טכנולוגיות ושיטות הגנה בתחום הגנת הסייבר. תכנון ארכיטקטורת רשת מאובטחת התואמת לצרכים הארגוניים וכמענה לאיומים הנשקפים ממרחב הסייבר. בחינת טכנולוגיות ומוצרי הגנה ושילובם בתשתיות המחשוב, לרבות מערכי אחסון ושיטות גיבוי והתאוששות מפגיעה. כתיבת מסמכי הקשחה והגנה למרכיבי הרשת (מערכות הפעלה, בסיסי נתונים, רשת תקשורת, אפליקציות, מסדי אחסון, עמדות הקצה, הצפנה ועוד). תכנון מערכות ניטור פיקוח והתראה הביטחוני כמענה לצורכי מרכז ניטור. ליווי הטיפול באירועי סייבר בהיבט הטכנולוגי והתהליכי.

### 1.11.2. הכשר ביטחוני לרמה 1 בתוקף.

### 1.12. דרישות נוספות בנושא השכלה וניסיון בדגש לניסיון Hands On :

- א. יכולת מוכחת בכתיבה ותכנון ארכיטקטורת אבטחת מידע והגנה בסייבר במערכות גדולות ומורכבות. (15%).
- ב. יכולת מוכחת בכתיבה, תכנון וביצוע SATP במערכות, יישומיים ותשתיות מידע מורכבות (17%).
- ג. יכולת מוכחת וניסיון עם יישומים, פיתוח קוד מאובטח, קוד פתוח ובדיקתם (10%).
- ד. ניסיון עם מימוש היבטי אבטחה בטכנולוגיות מערכי אחסון ווירטואליזציה (5%).
- ה. ניסיון במתן פתרונות הקשחה למערכות הפעלה ובדיקתם - Win Linux, (5%).
- ו. ניסיון ביטחוני טכנולוגי בנושא מחשוב מקבילי (צביר Cluster), מערכות הפעלה Linux/ Unix (10%).
- ז. ניסיון בכתיבת הנחיות אבטחה והקשחה של ציוד תקשורת: נתבים, מתגים פרוטוקולי תקשורת ופרוטוקולי ומנגנוני צפנה (10%).
- ח. ניסיון במימוש טכני בהטמעת מוצרי אבטחת מידע (5%).
- ט. ניסיון בהטמעת פתרונות לניהול משתמשים והרשאות (4%).
- י. ניסיון בביצוע בפועל של בדיקות חוסן וחדירה לאתרים (1%).
- יא. ניסיון בתחום End Point Security (3%).
- יב. ניסיון והכרות עם תחום תשתיות ושירותי מחשוב ענן (3%).
- יג. ניסיון בניתוח סיכונים במ"ם וסיוע בבחינת חלופות (2%).

## בלמ"ס

ד. ניסיון עם עולם ה-ERP, BI, DRP בדגש על מימוש היבטי הביטחון  
ואבטחת מידע(2%).  
טו. ידע בעולם התוכן הרלוונטי של הוא"א (8%).

1.13. אישורים מיוחדים נדרשים: על נותן השירות שייבחר, לעמוד בדרישות  
הביטחון כתנאי להוצאת ההזמנה ולתחילת מתן השירותים.

### 2. אופן הגשת ההצעה:

2.1. את ההצעה חובה להגיש על גבי נספח "מענה החברה" המצורף בנספח ג'  
בהודעת מכרז מרכזי: מ.16.2.11.

2.2. יובהר בזאת כי המציע חייב להשיב לפנייה. אם למציע אין נותני שירותים  
העונים על דרישות התפקיד - עליו לפרט בתשובתו את הסיבות לאי הגשת  
הצעה ואת האמצעים שהשקיע בניסיון לתת מענה.

2.3. המציע יצרף עבור כל מועמד אותו מציע טופס התחייבות מועמד המצורף  
בנספח "מענה החברה".

2.4. **חובה** לצרף קורות חיים + ת.ז. ואישורים בפירוט מלא על פי דרישות פנייה  
זו בהתייחס לכל אחד מהמועמדים.

2.5. חובה לצרף אישורים על השכלה עבור כל מועמד, הכוללים צילום תעודות  
המעידות על לימודים אקדמיים וכל לימודים וקורסים אחרים בתחום  
המחשוב ואבטחת המידע.

2.6. **הצעת המחיר** של הספק הינה התעריף לשעה שישולם לספק עבור שעת  
עבודה של המועמד. תעריף זה לא יעלה על התעריף המרבי לשעה כאמור  
בסעיף 1.5 לעיל.

2.7. הצעות הספקים לגבי המועמדים תוגשנה לתיבה שממוקמת בשער שורק,  
המרכז למחקר גרעיני יבנה, אשר תסומן כ"תיבת קבלת הצעות למועמדים  
מס' 30/2022". ההצעות תוגשנה במעטפות סגורות ללא ציון פרטי הספק או  
כל סימן זיהוי חיצוני אחר מלבד מספר הפניה.

### 2.8. אופן הגשת ההצעות:

יש להגיש מעטפה אחת (הכוללת 2 מעטפות) ולציין את מספר הפנייה:

2.8.1. **מעטפה אחת** - תשובה למרכיבי האיכות הדורשים מענה, כולל  
קורות חיים של נותני השירותים המוצעים מטעם הספק, בהתאם  
לפנייה זו.

## בלמ"ס

- 2.8.2. **מעטפה שנייה** - תשובה למרכיב העלות, בהתאם לפנייה זו. ספק רשאי להציע מחיר הנמוך מהמחיר המרבי הנקוב בסעיף 1.5 לפנייה זו.
- 2.9. הצעות אשר תגענה לתיבת המכרזים לאחר המועד המופיע בפניית המשרד עלולות שלא לבוא לדיון ולשקלול.
3. המשקל הכולל של מרכיב האיכות יהיה **70%** (באחוזים) ושל מרכיב העלות **30%** (באחוזים). הצעה שתפחת מציון 70% במרכיב האיכות - תיפסל.
4. ספק שיזכה לא יהיה רשאי לסגת מהצעתו, אלא אם לא ניתנה הודעה על זכייה בעקבות פנייה זו תוך 60 יום מהמועד האחרון להגשת ההצעות.
5. המשרד, על פי שיקול דעתו ומנימוקים שיפורטו, רשאי לדחות את כל המועמדים שהוגשו לו ולבצע פנייה מחדשת לכל הספקים הזוכים למתן מועמדים אחרים מאלו שהוצעו על ידם בפנייה המקורית.
6. לצורך שאלות וברורים ניתן לכתוב הודעת דואר אלקטרוני לכתובת ilanaf@mail.gov.il, עד תאריך 22/09/2022.
7. **המועד האחרון להגשת הצעות נקבע לתאריך 27/10/2022 עד השעה 13:00.**

