# נספח א2-מידע הנדרש להוכחת עמידה בתנאי הסף

**ניסיון המציע**

1. בטבלה **שלהלן** יש לפרט ארגונים להם סיפק המציע שירותי ייעוץ בכל אחד מהתחומים בהם הציע את מועמדותו.

לצורך הוכחת העמידה בתנאי הסף יש לפרט ניסיון בכל אחד מן השירותים המפורטים בסעיפים 2.1-2.3 בחלק ד' של מסמכי המכרז, בהיקף של 2000 שעות לפחות בכל שנה בכל סעיף, במהלך השנים 2023 ו -2024. לצורך ציון האיכות ניתן לפרט ניסיון נוסף בנספח א'3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **שם הארגון** | **תחום שירות הייעוץ (יש לסמן V)** | **מס' שעות בשנה** | **מועד מתן השירות****(חודש ושנה)** | **שם איש קשר אצל הלקוח, תפקיד ומס' טלפון עדכני**  |
|  | * שרותי מודיעין סייבר
* שירותי מבדקי סייבר טיפול באירועי סייבר, תצורת הגנה וטכנולוגיה
* מתודולוגיות הגנת סייבר, ארכיטקטורה, אסטרטגיה, מדיניות ונהלים, GRC
 |  |  |  |
|  | * שרותי מודיעין סייבר
* שירותי מבדקי סייבר טיפול באירועי סייבר, תצורת הגנה וטכנולוגיה
* מתודולוגיות הגנת סייבר, ארכיטקטורה, אסטרטגיה, מדיניות ונהלים, GRC
 |  |  |  |
|  | * שרותי מודיעין סייבר
* שירותי מבדקי סייבר טיפול באירועי סייבר, תצורת הגנה וטכנולוגיה
* מתודולוגיות הגנת סייבר, ארכיטקטורה, אסטרטגיה, מדיניות ונהלים, GRC
 |  |  |  |
|  | * שרותי מודיעין סייבר
* שירותי מבדקי סייבר טיפול באירועי סייבר, תצורת הגנה וטכנולוגיה
* מתודולוגיות הגנת סייבר, ארכיטקטורה, אסטרטגיה, מדיניות ונהלים, GRC
 |  |  |  |
|  | * שרותי מודיעין סייבר
* שירותי מבדקי סייבר טיפול באירועי סייבר, תצורת הגנה וטכנולוגיה
* מתודולוגיות הגנת סייבר, ארכיטקטורה, אסטרטגיה, מדיניות ונהלים, GRC
 |  |  |  |
|  | * שרותי מודיעין סייבר
* שירותי מבדקי סייבר טיפול באירועי סייבר, תצורת הגנה וטכנולוגיה
* מתודולוגיות הגנת סייבר, ארכיטקטורה, אסטרטגיה, מדיניות ונהלים, GRC
 |  |  |  |
|  | * שרותי מודיעין סייבר
* שירותי מבדקי סייבר טיפול באירועי סייבר, תצורת הגנה וטכנולוגיה
* מתודולוגיות הגנת סייבר, ארכיטקטורה, אסטרטגיה, מדיניות ונהלים, GRC
 |  |  |  |
|  | * שרותי מודיעין סייבר
* שירותי מבדקי סייבר טיפול באירועי סייבר, תצורת הגנה וטכנולוגיה
* מתודולוגיות הגנת סייבר, ארכיטקטורה, אסטרטגיה, מדיניות ונהלים, GRC
 |  |  |  |

1. בטבלהשלהלןיש לפרט את ניסיון העובדים הקיימים של המציע בתחום הגנת הסייבר. לצורך עמידה בתנאי הסף, יש לציין שמות של 4 עובדים העוסקים בתחום וכל אחד מהם בעל 7 שנות ניסיון מקצועי ומעלה.

|  |  |  |
| --- | --- | --- |
| **פירוט הניסיון בתחום הגנת הסייבר** | **מספר שנות הנסיון בתחום הגנת הסייבר (יש לסמן V)** | **שם העובד**  |
|  | * בעל 7 שנות ניסיון מקצועי ומעלה
 |  |
|  | * בעל 7 שנות ניסיון מקצועי ומעלה
 |  |
|  | * בעל 7 שנות ניסיון מקצועי ומעלה
 |  |
|  | * בעל 7 שנות ניסיון מקצועי ומעלה
 |  |

1. לצורך עמידה בתנאי סף 3.4, יש לפרט את פרטי מענה הטלפוני

|  |  |  |
| --- | --- | --- |
| **מספר טלפון** | **ימי פעילות** | **שעות פעילות** |
|  |  |  |
|  |  |  |

# נספח א3-מידע הנדרש להוכחת איכות ההצעה

1. גודל החברה וניסיון העובדים:

בטבלהשלהלןיש לפרט את ניסיון העובדים הקיימים של המציע בתחום הגנת הסייבר מעבר לנדרש בתנאי הסף, יש לציין שמות של עובדים העוסקים בתחום, וכן את מספר שנות נסיון שלהם בתחום הגנת הסייבר.

|  |  |  |
| --- | --- | --- |
| **פירוט הניסיון בתחום הגנת הסייבר** | **מספר שנות הנסיון בתחום הגנת הסייבר** | **שם העובד**  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. מומחיות ייחודית:

יש לציין מומחיות ייחודית של החברה. יש לפרט את הדברים הבאים לפי החלוקה שלהלן:

* 1. פעולות, כלים או מתודולוגיות, שבאמצעותם החברה יכולה לתת שירות מיוחד לבנק ישראל ו/או ערך מוסף.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

* 1. **יש לפרט ניסיון רלוונטי במערכות זהות/דומות למערכות הקיימות בבנקים או בבנק מרכזי.**

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

1. המלצות:

בטבלהשלהלןיש לפרט את פרטיהם של 5 לקוחות מהשנים האחרונות:

|  |  |  |  |
| --- | --- | --- | --- |
| **פרטי איש קשר (טלפון וכתובת מייל):** | **השנים בהן בוצעה ההתקשרות עם הארגון** | **ארגון** | **שם הממליץ** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |