מכבי שירותי בריאות

*מחלקת רכש ציוד וחומרים*

**בקשה להצעת מחיר לרכישה, יישום, והטמעת מערכת חיתום דיגיטלי**

**ושמירת מפתחות (HSM) בתצורה היברידית**

## 1. כללי:

1.1. מכבי שירותי בריאות (להלן - **"מכבי"**) מעוניינת לקבל הצעות מחיר לרכישה, יישום והטמעת מערכת חיתום דיגיטלי ושמירת מפתחות (HSM) בתצורה היברידית. (להלן – **"המערכת"**).

1.2. הקמת התשתית תכלול רכיבי HSM, הקמה, תיעוד מלא, ואינטגרציה עם מערכות מכבי ומערכת לחיתום מרכזי, כמפורט בבקשה.

1.3. הפתרון אשר יוצע ע"י ספק הפתרון יעמוד בכל דרישות נוהל 107 של משרד הבריאות: "מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי".

1.4. את ההצעות יש לשלוח אל שרון ויצמן לדוא"ל: waizman_sh@mac.org.il עד לתאריך **24.07.2023**

1.5. מכבי שומרת לה הזכות לנהל מו"מ עם הספק המוביל ולסכם את פרטי העסקה בשילוב היצרן.

1.6. מכבי אינה מתחייבת לקבל את ההצעה הזולה ביותר, חלק מההצעה או כל הצעה שהיא.

1.7. ספקים עמם תתקשר מכבי, יחתמו על ההסכם לבקשה תוך 7 ימים מקבלת הודעה על רצונה של מכבי להתקשר עמם. מסמכי הבקשה והצעת הספק יהוו חלק בלתי נפרד מהסכם ההתקשרות שייחתם.

1.8. שאלות בנושאים טכנולוגיים יש להפנות אל חן וולף שחם במייל wolf_c@mac.org.il

## 2. תהליך הבחינה של ההצעה:

2.1. עלות ההצעה

2.2. עמידה בדרישות והתאמה לצרכי מכבי

2.3. הספק כחברה – יציבות כלכלית, יכולת לספק את העבודה וצוות המומחים למתן השירותים הנדרשים

2.4. המלצות מלקוחות

**להלן פירוט המשקולות לבחינת ההצעות:**

| | | |
|---|---|---|
| **עלות** | **60%** | |
| עלות המערכת בהתאם לבל"מ | 100% | |
| **סה"כ עלות** | **100%** | |
| **איכות** | **40%** | **ציון סף מינימלי** |
| עמידה בדרישות והתאמה לצרכי מכבי כפי שמפורט בסעיף 4 | 80% | 80% |
| ניסיון בהתקנה של המוצר המוצע, 3 התקנות לפחות בשנתיים האחרונות בתצורה דומה בארגונים גדולים (1000 משתמשי קצה לפחות) | 10% | 80% |
| ניסיון כוח האדם המוצע לפרויקט זה בהתאם למפורט במסמכי הבל"מ. יתקיים ראיון טכני עם מומחה הספק והתרשמות מיכולותיו | 10% | 80% |
| **סה"כ איכות** | **100%** | |

**ציון איכות הנמוך מציון הסף המינימלי, יפסול את הצעת המציע.**

3. **<u>תיאור המצב הקיים (בנושא חתימה על מרשמים)</u>**

<u>רקע ותיאור כללי:</u>

קופ"ח מכבי מונה מעל 2 מיליון חברים, המקבלים שירותים רפואיים שונים בכ – 300 מרכזים רפואיים ובלמעלה מ - 100 בתי מרקחת. השירותים ניתנים במהלך כל ימי השבוע 24/7 בין השעות 06:00 ל 24:00. מופקים מספר רב של מסמכים דיגיטליים על ידי רופאי מכבי. הרופא עובד על מערכת התיק הרפואי (להלן: "קליקס") ומפיק מרשמים באמצעות מערכת זו. כיום הקליקס עובד מול פתרון החיתום הקיים מתוך הפעלת DLL מתווך שפותח על ידי היצרן ובקליקס בוצע פיתוח שיפעיל את ה-DLL.

המוצר הקיים כיום DOCUSIGN מגיע ל EOL וכתוצאה מכך מכבי מעוניינת לבחון חלופה למוצר הקיים.

4. **<u>תכולת הבקשה</u>:**

4.1. מערכת חיתום מרכזית שתשמש את רופאי מכבי לחיתום על מרשמים דיגיטאליים. המערכת תכלול התקנת שרתי HSM והגדרתם בצורה שיתממשקו למערכת התיק הרפואי של מכבי.

4.2. הפתרון יתמוך באחסון מפתחות בתצורה היברידית – ענן ו- on prem (HSM) .

4.3. פתרון חיתום מרכזי Trustworthy System Supporting Server Signing (TW4S) יכלול:

4.3.1. רכיב מאובטח לניהול מחזור חיי מפתחות החיתום כדוגמת HSM. שירות חיתום רשתי מרכזי מאובטח - תוכנה Trusted Signature Creation Module הרצה על שרת ברשת, ותומכת בחותמים מרוחקים לחיתום מרחוק על מסמכים, תוך שימוש במפתחות חיתום הנשמרים באופן מאובטח וניתנים לשליטת בעל המפתח בלבד.

התוכנה תכלול כמינימום את הפונקציות הבאות:

4.3.1.1. זיהוי המשתמש (באופן שיפורט בהמשך).

4.3.1.2. אתחול ה- SCD (Signature Creation Data) לאתחול מפתחות חתימה.

4.3.1.3. חיתום דיגיטאלי.

4.3.2. API לפיתוחים עתידיים.

4.3.3. תוכנת Client הכוללת Cryptographic Service Provider וכל רכיב נדרש אחר לביצוע חיתום מרוחק.

4.3.4. תמיכה בתהליכי מחזור חיי תעודה דיגיטאלית (הנפקה, ביטול, חידוש).

4.3.5. ביצוע מעבר שקוף ממערכת נוכחית למערכת החדשה בצורת החלפת ה-DLL.

4.3.5.1. העברת מסמכים שונים לחתימה ולכל מסמך יוגדר המיקום של החתימה (קואורדינטות: X,Y).

4.3.5.2. חלק מהמסמכים יחתמו אך לא תוטבע להם החתימה.

4.3.5.3. במקרים של כשל בחתימה, הDLL יחזיר קוד שגיאה + טקסט המסביר את השגיאה.

4.3.5.4. מצ"ב פרטי DLL קיים:

| CLICKS | DLL |
|---|---|
| תמיד 1 | add key="page" ><br></"value="1 |
| שם טופס | </" מרשמים "=add key="reason" value> |
| מיקום החתימה X ( פיקסלים ) | </"add key="x" value="101> |
| מיקום החתימה Y ( פיקסלים ) | </"add key="y" value="101> |
| גודל החתימה "גובה" | </"add key="height" value="200> |
| גודל החתימה "אורך" | </"add key="width" value="300> |
| הצגה / אי הצגה של החתימה | </"add key="include_logo" value="true> |

| CLICKS | DLL |
|---|---|
| | |
| לא בשימוש | </"add key="invisible" value="false> |
| לא בשימוש | </"add key="reason" value="11111111>הנני מאשר בחתימתי מרשם זה |
| לא בשימוש | </"add key="include_reason" value="true> |
| לא בשימוש | </"add key="include_signing_time" value="true> |
| לא בשימוש | </"add key="include_graphical_image" value="true> |
| לא בשימוש | </"add key="include_signer_name" value="true> |

4.3.5.5. רכיב שני On Prem שיענה על דרישות DRP. 2 appliances יושבים בשני אתרים שונים ומגבים אחד את השני בתצורת active / active

4.3.5.6. אחסון תעודות דיגיטליות על גבי שרת החיתום המרכזי שעומד בתקן FIPS140-2 Level 3

4.3.5.7. ניטור אירועים – נדרש לוג אירועים לכל שירותי המערכת

4.3.5.8. רכיב שלישי כגיבוי בענן (מיקום הענן ותצורת ה appliance ) – CLUSTER/עבודה במקרה כשל פניה לשירות הענני להמשך תפעולי.

4.3.5.9. PKI – למכבי קיימת תשתית PKI. שעל גבי תשתית זו יממוש הפתרון. הפתרון אמור בפועל לנהל את התעודות האלה ולבצע באמצעותן את החתימה ולטובת זה נדרש CA. אותו CA יהיה Subordinate של ה- Root CA הארגוני. המפתחות יוחזקו ב-HSM

## 5. <u>ארכיטקטורה</u>

5.1. HSM - רכיב המשלב חומרה ותוכנה, המיועד לחילול ושמירה של מפתחות הצפנה. ברכיב זה יאוחסנו המפתחות הפרטיים של שרתי ה- CA באופן שיבטיח את אבטחתם ושלמותם.

5.1.1. התחנה מקושרת לשרת טרמינל מולו היא מזדהה. מערכת קליקס עובדת על שרתי CITRIX רופא מבקש לחתום על מרשם באמצעות קליקס מרכזי.

5.1.2. רופא מבקש לחתום על מרשם באמצעות קליקס מרכזי.

5.1.3. עולה מסך הזדהות בו מקיש הרופא שם משתמש AD, סיסמת AD וסיסמת OTP. מתבצע זיהוי רדיוס (קיים במכבי) לסיסמת ה- OTP ואחריה זיהוי ל-AD.

*כיום ההזדהות היא מול ה-AD בלבד ללא OTP

5.1.4. בקשת החתימה מועברת מקליקס לממשק (DLL) שיפתח הספק ויתואר בהמשך.

5.1.5. דרישות משירות החיתום המרכזי מפורטות במסמך זה. כמו כן השירות עשוי לכלול מספר שרתים ושירותים נפרדים או בהתקן יחיד.

5.1.6. תחנות ניהול והנפקה ישמשו את המנפיקים וגופי התמיכה.

5.1.7. מכונות החיתום נדרשות להיות CA בפני עצמן. אך כפי שנכתב אמורות להיות כחלק מתשתית PKI הארגוני וכפופות ל-ROOT CA הארגוני. ניתן לעשות בו שימוש או להציע חלופות.

5.1.8. לכל הרופאים User ב-Domain.

5.2. הקשר בין תשתית ה-PKI לשרת החיתום:

הפתרונות המוצעים יכללו קשר בין תשתית החיתום לתשתית ה-PKI.

5.2.1. תעודות החתימה יונפקו משרת Subordinate CA שיחתם על ידי ה- Root CA. שרת זה יכול להיות חלק ממערכת החיתום או שרת מיקרוסופט שמהווה חלק מהתשתית.

5.2.1.1. באמצעות ממשק ניהול בשרת החיתום ייחולל צמד מפתחות (פרטי וציבורי) ובקשה לתעודה תישלח לשרת ה- CA בשם החותם.

5.2.1.2. CA יחתום על הבקשה ויחזיר תעודה.

5.2.1.3. התעודה תותקן בשרת החיתום באופן אוטומטי.

5.2.1.4. בעת חידוש תעודה תוגש בקשה אוטומטית משרת החתימות לשרת ה- CA

5.2.1.5. הדגש הוא שניהול התעודות יבוצע באופן שקוף ע"י מערכת החיתום.

5.2.2. בכל אחד מהמקרים תעודת החתימה תהיה תחת היררכית מכבי.

## 6. מפרט טכני של הדרישות משרת החיתום המרכזי

### 6.1 תשתיות

| מס"ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| 6.1.1 | פתרון חיתום מרכזי המתבסס על התקן הכולל בתוכו את כל המרכיבים הנדרשים למימוש הפתרון או חלוקת פונקציות בין שרתים בין מספר שרתים | חובה | |
| 6.1.2 | הפתרון ישתלב בסביבת Active Directory קיים במכבי לטובת הגדרת הרשאות, קבוצות הנפקה והזדהות | חובה | המציע יתאר את מערכת ההרשאות למוצר |
| 6.1.3 | הפתרון ישתלב בסביבת PKI הקיימת בארגון | חובה | |
| 6.1.4 | יתירות ברמת רשת וספק כוח | חובה | |
| 6.1.5 | Rack mounted באופן שניתן להתקנה בארונות תקשורת סטנדרטים בחדר השרתים | חובה | |
| 6.1.6 | סנכרון זמן: יש לסנכרן את מערכת החיתום עם מקור זמן סטנדרטי של מכבי | חובה | |
| 6.1.7 | Scalability - יש לתאר אפשרות להרחבת המערכת לשיפור ביצועים ושרידות למשל Load Balancing | חובה | המציע יתאר האם ניתן להרחיב לעוד שרתי הנפקה כדי לשפר ביצועים |

### 6.2 פיתוחים

| מס"ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| 6.2.1 | זיהוי: משתמש יקיש User וסיסמת AD ובנוסף שדה OTP. המערכת תבדוק תחילה את ה- OTP ולאחר הצלחה את זיהוי ה- AD.<br>נדרשת תמיכה מלאה בזיהוי מבוסס OTP (המחולל במכשיר סלולארי או נשלח אליו) אותו מקיש המשתמש. הטכנולוגיה הקיימת במכבי מבוססת שרת Vasco שפועל כרדיוס | חובה | ר' 5.1.4 |
| 6.2.2 | DLL שיספק את הממשק הבא: | לידיעה | |
| | פונקציית חתימה sign(path, appearance)<br><br>הקליקס טוען את תכנית ההחתמה ושולח:<br><br>path = of file to sign [string]<br><br>example: | חובה | |

| | | | |
|---|---|---|---|
| | path = "C:\Documents and Settings\gal_sa\Local Settings\Temp\12300001.pdf"<br><br>Appearance = signature appearance [string]<br>Example:<br>Appearance = "clicks_pr"<br>הפונקציה תחזיר קוד 0 בהצלחה<br>וקודים אחרים לכישלון (רשימה תועבר בשלב האפיון) | | |

### 6.3 ביצועים

| מס״ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| 6.3.1. | יכולת חיתום של 100-150 חותמים בו זמנית | חובה | |
| 6.3.2. | זמן ביצוע חתימה אחת לא יעלה על 1 שניה מרגע שמגיע לשרת החיתום (הזמן בתוך שרת החיתום). | חובה | |

### 6.4 אבטחת מידע

| מס״ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| 6.4.1. | הפתרון המוצע יספק מענה לדרישת חוק החתימה האלקטרונית 2001 שם נכתב כי חתימה אלקטרונית מאובטחת הופקה באמצעי הניתן לשליטתו הבלעדית של בעל אמצעי החתימה | חובה | הספק יוכיח כיצד שליטת בעל אמצעי החתימה מתקיימת בהתקן מרכזי כפי שקורא בכרטיס חכם. |
| 6.4.2. | **פתרון החיתום המרכזי יתמוך בבעלי תפקידים הבאים:** | לידיעה | יש לתאר את מערכת הרשאות תפקידי הניהול וכיצד ניתן לממש את הפירוט הבא |
| 6.4.3. | תמיכה ב- RBAC – Role Base Access Control ל- HSM לבעלי התפקידים השונים בארגון.<br>הדרישה שתהיה תמיכה בביזור סמכויות כך שלא ניתן יהיה לתפעל את ה- HSM ברמה של חתימה על שרתים ע״י בעל תפקיד יחיד | לידיעה | |
| 6.4.4. | **קצין אבטחה** : אחראי על ניהול ומימוש מדיניות אבטחת המידע במוצר | חובה | |
| 6.4.5. | **מנהל מערכת** : מורשה להתקין, לקנפג ולתחזק את המערכת, תוך הגבלת הרשאות לפרמטרי א״מ | חובה | |
| 6.4.6. | **מפעיל המערכת** : פעילות שוטפת כגון גיבוי ושחזור המערכת | חובה | |

| | | | |
|---|---|---|---|
| .6.4.7 | **מבקר המערכת**: מורשה לצפות בלוגים, ואירועים. | חובה | |
| .6.4.8 | ניתן יהיה לשייך משתמשים לתפקידים הנ"ל | חובה | |
| .6.4.9 | המערכת תוודא שמשתמש שמוגדר כפקיד אבטחה אינו מורשה כמבקר | יתרון | |
| .6.4.10 | המערכת תוודא שמשתמש שמוגדר כמנהל המערכת אינו מורשה כמבקר או פקיד אבטחה. | יתרון | |
| .6.4.11 | בשום מקרה לא יוכל בעל תפקיד ניהולי במערכת לחתום בשם משתמש אחר | חובה | יש לפרט כיצד ממומשת דרישה זו |
| .6.4.12 | יש למסור דו"ח בדיקות של בודק חיצוני הכולל בדיקות אבטחת קוד, בדיקות פריצה ובדיקות אבטחת התהליכים | יתרון | |
| .6.4.13 | פירוט יכולות התממשקות דרך רכיבי אבטחת מידע (DataPower, Netscaler, F5 וכד') | חובה | |
| .6.4.14 | שירותי הענן ב region EU, ככל שהמערכת מבוססת ענן ציבורי | חובה | |
| .6.4.15 | התממשקות לוגים למערכת SIEM של מכבי – QRADAR | חובה | |
| .6.4.16 | תמיכה ב SSO מבוסס AZURE AD - SAML/OAUTH | חובה | |
| .6.4.17 | יש להפריד HSM ברשת פרטית | לידיעה | בתלות בארכיטקטורה שתיבחר, אם תהיה הפרדת רשתות, יהיה צורך בממשק רשת נוסף עבור כל CA ותחנת ניהול בסגמנט חדש. |
| .6.4.18 | קביעת פרמטרי CA שיתאימו לאורך מפתח 4096 | חובה | |
| .6.4.19 | אורך מפתח תעודות קצה יהיה 2048 | חובה | |
| .6.4.20 | יש לתכנן פרמטרי תשתית לתמיכה בתעודות קצה של עד 6 שנים | חובה | |
| .6.4.21 | יש לכלול בפתרון נוהל Key Ceremony שכולל גם את אופן הפרדת הרכיבים של שמירת הסודות השונים בין כפסות שונות | חובה | |
| .6.4.22 | כל התקשורת עם ה- HSM תהיה מוצפנת | חובה | |
| .6.4.23 | מניעת יכולת העתקת מפתח פרטי מה-HSM | חובה | |
| .6.4.24 | נדרשת תמיכה בסטנדרטים כגון CAPICOM, PKCS#11 | חובה | |

### 6.5. הזדהות

| מס"ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| 6.5.1. | בעת ביצוע חתימה יתבקש המשתמש להציג נתוני הזדהות | חובה | |
| 6.5.2. | הפתרון המוצע יתמוך בשיטות ההזדהות הבאות: | ידיעה | |
| 6.5.3. | הזדהות שם משתמש וסיסמת Active Directory **של מכבי** | חובה | |
| 6.5.4. | הזדהות OTP מבוסס טוקני Vasco הקיימים במכבי (Radius) או כל פתרון אחר שתומך ב-Radius | חובה | |
| 6.5.5. | זיהוי OTP שישלח כ- SMS ע"י תשתית הקיימת במכבי או יחולל במכשיר סלולארי (באחריות מכבי). התשתית כוללת התקן ומנגנון משלוח הודעות SMS. | חובה | |
| 6.5.6. | לאחר פרק זמן שיקבע כפרמטר ע"י מכבי יידרש זיהוי מחדש. באותו פרק זמן החיתום יתבצע על בסיס הזיהוי האחרון. | חובה | |
| 6.5.7. | במקרה של מספר כישלונות בזיהוי שיקבעו כפרמטר, המערכת תמנע אפשרות זיהוי נוסף לפרק זמן שיקבע כפרמטר | חובה | |
| 6.5.8. | זיהוי מחודש יידרש לאחר ביצוע Logout | חובה | |

### 6.6. ניהול ותפעול

| מס"ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| 6.6.1. | יסופקו מדריכי ניהול ותפעול למערכת שיכללו: | לידיעה | |
| 6.6.2. | מדריך התקנה וניהול | חובה | הוראות התקנה, אבטחת המוצר, תקלות נפוצות ופתרונן. |
| 6.6.3. | מדריך שימוש | חובה | |
| 6.6.4. | ממשק ניהול אינטואיטיבי ופשוט לתפעול ה-HSM | יתרון | |

### 6.7 ניהול מפתחות

| מס"ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| 6.7<br>6.7.1 | מפתחות חיתום משתמש יחוללו רק בהתקן ייצור החתימות (HSM) אמצעי זה יעמוד בתקן FIPS 140-2 level 3 | חובה | |
| 6.7.2 | אמצעי חילול המפתחות יתמוך באלגוריתמים קריפטוגרפים ואורכי מפתחות המצוינים בהנחיית רשם הגורמים המאשרים מס' 4/2010 "עדכון אלגוריתמים ואורכי מפתחות" | חובה | ניתן למצוא הנחיה זו בלינק הבא: http://index.justice.gov.il/Units/ilita/LawInfo/Hanchayot/HanchayotBetokef/Pages/HanhayotCA.aspx |
| 6.7.3 | מפתחות פרטיים ישמרו תמיד באופן מאובטח שיבטיח סודיות ומהימנות המפתחות | חובה | |
| 6.7.4 | ניהול מחזור חיי מפתחות החותמים יבוצע באמצעות תוכנת ניהול שרת החתימות באופן אוטומטי , כך שלא תידרש רכישת מערכת ניהול נוספת חיצונית | חובה | |
| 6.7.5 | גיבוי מפתחות פרטיים יתבצע באופן מאובטח שיבטיח סודיות ומהימנות המפתחות | חובה | |
| 6.7.6 | מפתחות בקרה (זיהוי מנפיקים למשל) ותשתית (למימוש הצפנת SSL למשל) ישמרו על גבי ה-HSM | יתרון | |
| 6.7.7 | יש לאפשר חידוש מפתחות בקרה ותשתית על בסיס תקופתי | יתרון | |

### 6.8 ניטור

| מס"ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| 6.8.1 | יש לכתוב ללוג את האירועים הבאים: | חובה | |
| 6.8.1.1 | אירועי ניהול מפתחות (לפחות חילול, מחיקה, פגי תוקף) | חובה | |
| 6.8.1.2 | חיתום מוצלח שיכלול זהות החותם | חובה | |
| 6.8.1.3 | הדלקה וכיבוי של מנגנון ה-Audit | חובה | |
| 6.8.1.4 | שינוי פרמטרי Audit | חובה | |
| 6.8.2 | יש להגן על מנגנון ה-Audit מפני שינוי ומחיקה | חובה | |
| 6.8.3 | פריט Audit יכלול: זמן ושעה, סוג האירוע, אחראי על הפעולה, הצלחה / כישלון. | חובה | |

| | | | |
|---|---|---|---|
| .6.8.4 | פורמט נתוני הביקורת יהיה קריא | חובה | |
| .6.8.5 | ינוהל לוג אחד למערכת כולל תתי המערכות וירשם ל-EventLog של השרת או במקרה של התקן (device) ייתמך פרוטוקול Syslog | חובה | יש לפרט מבנה לוג |
| .6.8.6 | המערכת תפיק התראות Warnings בעת קרות אירועי אבטחת מידע כגון: חיתום מחוץ לשעות פעילות שיוגדרו, חיתום בקצב גבוה מידי, פתיחת יותר מ- Session יחיד מאותו משתמש, ניסיונות גישה לא מורשית למערכת | חובה | |
| .6.8.7 | תמיכה בפרוטוקול SNMP בגרסה 3 (Trap) | חובה | |
| .6.8.8 | יש לשלב את הפתרון עם מערכות הניטור המרכזיות של מכבי | חובה | יסופקו פרטים בשלב האפיון |
| .6.8.9 | HSM - ניטור הפעילויות שלהלן כמינימום נדרש: נפילה והעלאה פעולות ייצור מפתחות, התחברות משתמש, כישלונות זיהוי, קריאה ומחיקת לוג, ניסיון Tamper, שינוי קונפיגורציה | חובה | על הספק לתאר יכולות ניטור נוספות של המערכת - יתרון |
| .6.8.10 | CRL לא פורסם | חובה | |
| .6.8.11 | CRL אינו תקף או לא נמצא בנקודת הפרסום | חובה | |
| .6.8.12 | ניטור פגות תוקף של תעודות ומחצית חיים של כל התעודות בשרתי CA | חובה | |
| .6.8.13 | ניטור והתרעה על פגי תוקף תעודות קצה | יתרון | ספק הפתרון רשאי להציע מוצר מדף דרך צד ג'. |

### .6.9 גיבוי ושרידות

| מס''ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| .6.9.1 | גיבוי פרמטרי אבטחה ומפתחות המערכת יהיה מוצפן וחתום | חובה | |
| .6.9.2 | יינתן מנגנון שחזור שישחזר את מצב המערכת לנקודת הגיבוי | חובה | |
| .6.9.3 | High Availability Clusters - יכולת מובנית לזמינות גבוהה במודל Active/Active . | חובה | |
| .6.9.4 | יש לכתוב נוהל גיבוי שיכלול פריטי מידע שיש לגבות כדי לבצע שחזור של תשתית לאחר נפילה | חובה | |
| .6.9.5 | שירות CRL - יהיה זמין ונגיש באופן מלא | חובה | |
| .6.9.6 | שירותי subordinate CA ניתן לשקם תוך 24 שעות | חובה | |

| | | | |
|---|---|---|---|
| .6.9.7 | שירותי subordinate Root CA ניתן לשקם תוך 14יום | חובה | |
| .6.9.8 | HSM – הספק יוכיח שיש ברשותו מכשירים חלופיים זהים או בעלי יכולות משופרות, למקרה של צורך בהחלפת מכשיר | חובה | |
| .6.9.9 | נדרשת יכולת גיבוי מלא של פרמטרי ההתקנה והתוכן השמור ב- HSM בצורה מוצפנת הגיבוי יהיה על אחסון ייעודי / כספות וימומש בהתאם לפתרון הנבחר | חובה | |

### .6.10 תקנים ורגולציות

| מס"ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| .6.10.1 | חיתום מאובטח - שירות החיתום המרכזי יתמוך בכל סעיפי מסמך "תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות) התשס"א-2001 | חובה | יש לספק חוות דעת משפטית התומכת בדרישה |
| .6.10.2 | עמידה בכל דרישות נוהל 107 (על נספחיו) של משרד הבריאות - "מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי". | חובה | דרישה זו מהווה דרישת סף. בפרק תהליכים נתמכים יפרט המשיב כיצד ממומשים תהליכי הנפקה במערכת |
| .6.10.3 | עמידה בדרישות תקן אירופאי CEN/prEN 419241-1:2014 | יתרון | במענה יש להציג עמידה בסעיפי פרק 6 בתקן. במידה והייתה התייחסות בסעיפים הקודמים יש רק להפנות לסעיף המתאים |
| .6.10.4 | עמידה בתקן FIPS 140-2 level 3 | חובה | יש לצרף תעודה ולפרט לאלו רכיבים ובאיזו תצורת מערכת ניתן התקן |

### .6.11 תהליכים נתמכים

| מס"ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| .6.11.1 | **תהליך רישום וזיהוי** : סעיף 3.1.4 בנוהל 107, כיצד המערכת מגבילה את כמות התעודות למשתמש לתעודה יחידה | חובה | |
| .6.11.2 | **אחריות והוראות כלליות** סעיף 3.2.5 בנוהל 107, נדרש סימון בתעודת החתימה שהיא מותקנת ע"ג שרת. | יתרון | |
| .6.11.3 | **הנפקה** : יש לפרט עמידה בדרישות סעיף 3.6.1 לנוהל 107 נספח א'. | יתרון | |
| .6.11.4 | **הנפקה** : ניתן להנפיק תעודה מתשתית PKI פנימית של מכבי באופן המתואר בסעיף 3.6.4- | יתרון | המציע יתאר בפירוט את תהליך ההנפקה של תעודת חתימה לרופא. בשתי שיטות : תוך |

| | | | |
|---|---|---|---|
| | 3.6.5 של נוהל 107 נספח א' | | שימוש בתשתית PKI שתוקם במכבי, תוך שימוש בתשתית PKI המגיע עם המוצר כולל צילומי מסך. |
| .6.11.5 | **הנפקה:** יש לתמוך בשיטות הנפקה אוטומטיות העונות על הדרישות. | חובה | במקרה זה יש לתאר כיצד ניתן להנפיק לקבוצת רופאים תעודות באופן שידמה הנפקת אצווה של כרטיסים עם PIN אקראי. רק הרופא יוכל לאחר זיהוי לאקטב את אמצעי החתימה. |
| .6.11.6 | **הנפקה מחדש:** תמיכה בחידוש אוטומטי תוך התבססות על התעודה התקפה הקיימת | חובה | יש לתאר תהליך בו תעודות מתחדשות על בסיס הקיימות עם או ללא התערבות המשתמש |
| .6.11.7 | **ניהול תעודות:** מוצר החיתום המרכזי ינהל את התעודות מבחינת התראה על פגי תוקף | יתרון | |

.6.12 **כתיבת נהלים –**

| מס"ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| .6.12.1 | **"כתבו הנהלים הבאים** | | |
| .6.12.1.1 | טקס חילול מפתחות | חובה | |
| .6.12.1.2 | נוהל גיבוי שחזור | חובה | |
| .6.12.2 | **"כתבו ההוראות הטכניות הבאות** | | |
| .6.12.2.1 | הקמת וקינפוג HSM | חובה | |
| .6.12.2.2 | גיבוי שחזור | חובה | |
| .6.12.3 | **"כתבו המסמכים הבאים** | | |
| .6.12.3.1 | אפיון טכני מפורט | חובה | |
| .6.12.3.2 | מסמך התאוששות מאסון | חובה | |

**6.13. שונות**

| מס"ד | דרישה | חשיבות | הערות |
|---|---|---|---|
| 6.13.1. | יכולת חתימה על הקבצים מהסוגים הרשומים מטה: | ידיעה | |
| 6.13.1.1. | PDF (תואם Adobe) | חובה | |
| 6.13.1.2. | Microsoft Office | יתרון | |
| 6.13.1.3. | TIFF באמצעות plugin | יתרון | |
| 6.13.1.4. | HTML | יתרון | |
| 6.13.1.5. | XML | יתרון | |
| 6.13.1.6. | דואר אלקטרוני Outlook | יתרון | |
| 6.13.1.7. | Share Point | יתרון | |
| 6.13.2. | למוצר יהיה API שיאפשר למפתחי מכבי להתממשק בעתיד למערכות ויישומים נוספים לשם ביצוע חתימות. הממשק יתמוך ב- | חובה | |
| 6.13.2.1. | שפות תכנות C# net. | חובה | |
| 6.13.2.2. | Java, VB , C\C++ | יתרון | |
| 6.13.2.3. | ממשק Web Service | חובה | |
| 6.13.2.4. | תוכנת Client | חובה | המשיב יתאר כל תוכנה הנדרשת להתקנה בצד ה-Client למימוש הפתרון |
| 6.13.2.5. | מבנה התעודה: יש להציג עמידה בדרישת נוהל 107 נספח ב סעיף 2.1.7 | חובה | |
| 6.13.3. | נדרשת תמיכה ותאימות לגרסאות מערכות הפעלה של מיקרוסופט. | חובה | |

## 7. <u>דרישות הטמעה ואינטגרציה:</u>

7.1. פרויקט החלפת והטמעת מערכת חיתום מרכזית חדשה במכבי, הינו מסוג Turn Key Project, בו המציע שיבחר, יספק פתרון העונה על כל דרישות מפרט זה, כולל פיתוח קובץ ה-

DLL, התקנה בסביבת Test במכבי ולאחר בדיקות קבלה, התקנה בסביבת ייצור ואינטגרציה עם מערכות קיימות, AD קליקס, Vasco.

7.2. על הספק לכתוב מסמכי SOW, LLD,HLD.

7.3. תינתן הדרכה לאנשי מכבי (לצוותים הטכניים המתחזקים במכבי) וליוויים בתקופת הטמעת המערכת.

7.4. ההטמעה תתבצע באופן מדורג תוך מינימום זמן השבתה. בהתאם לתוכנית עבודה מפורטת שתיכתב על ידי הספק.

7.5. הפעלת המערכות בסביבת הייצור, אשר דורשת השבתת המערכות, תתבצע החל מהשעה 23:00.

7.6. הדרכה ברמת מנהל מערכת (Administrator) לנציגי מערכות מידע של מכבי, יש צורך במדריך ברמת מומחה בעל ניסיון רב בהטמעת המוצר, ההדרכה תינתן לצוות אבטחת מידע של מכבי, תוכן ההדרכה יאושר ביחד עם מכבי.

7.7. אספקת תיעוד מלא למערכת לאחר סיום הטמעה (As made)

7.8. על הספק לצרף גאנט (GANTT) שיכיל את כלל השלבים המוצעים. על הספק לפרט בתוכנית העבודה את הפעילויות התלויות בספק ואת הפעילויות הנוספות שידרשו ממכבי (כדוגמת פעולות הכנה וכו'). על הגאנט לכלול גם אישורי מסמכים, סקרים פגישות סטאטוס וכו.

7.9. יש לתכנן סיום הפרויקט והתחלת הנפקת תעודות חיתום לרופאים בתחילת ספטמבר 2023.

## 8. <u>דרישות פיתוח:</u>

8.1. בסעיפים 5-6 מספר דרישות שייתכן שיהיה צורך לפתח ולשלב במוצר. למשל מנגנון מקביל ל-DLL הקיים היום בקליקס.

8.2. פיתוח יבוצע על פי מתודולוגית פיתוח מאובטח של מכבי ויהיה כפוף לסקר סיכונים ומבדקי חדירה לפי פרק 11 בהסכם.

8.3. בסיום הפיתוח יוצגו דו"חות בדיקות קוד וחדירה ע"י גוף חיצוני בלתי תלוי

8.4. הפיתוח יכלול תיעוד מלא: אפיון טכני מפורט ותיק תכנות

8.5. מסירת קוד מקור:

8.5.1. במועד סיום מבדקי הקבלה של כל רכיב מרכיבי מערכות הפרויקט, ימסור הספק למכבי את קוד המקור המתאים והמעודכן של הרכיב שפותח, לרבות כל התיעוד הרלוונטי לקוד המקור.

8.5.2. בכל מסירה כאמור, ימסור הספק סט שלם של תוכניות המקור של מערכות הפרויקט בכללותן, כפי שיהיו לאחר העדכון הרלוונטי, על גבי מדיה מגנטית ו/או אופטית וכן במסמך כתוב. קודי המקור יהיו קריאים ויכילו הערות והסברים באופן שתוכניתן סביר יוכל לעשות בהן שימוש מקצועי.

## 9. דרישות תחזוקה ותמיכה:

9.1. תמיכה לכלל המוצרים הכלולים בהצעה זו, לתקופת תחזוקה הכלולה בהצעה זו מיום האספקה בפועל.

9.2. תמיכה בכלל סוגי השרתים ומערכות הפעלה – Microsoft Windows 10 ומעלה, Windows Server 2019 ומעלה, MS-SQL2019, Citrix, Cockpit , לרבות תמיכה בגרסאות העתידיות של מערכות הפעלה ושרתים, קבלת עדכונים ושדרוגי גרסאות שוטפות ותמיכה בהתקנת השדרוגים.

9.3. תמיכה עתידית באפליקציות מכבי אשר נשענות על פתרון החיתום(דוגמת קליקס).

9.4. קבלת תמיכה ופתיחת קריאות במרכז התמיכה של היצרן, לפי הפירוט בסעיף SLA.

9.5. תמיכה וסיוע בהפעלת המערכת.

## 10. זמן תגובה נדרש (SLA) מהספק:

10.1. לתקלות רגילות - תמיכה טלפונית לפי שעות עבודה בזמן ישראל, לכל היותר NBD

10.2. במידה והבעיה לא נפתרת תהיה אפשרות לנציג מכבי להעלות את רמת החומרה.

10.3. תקלה משביתה תיקבע על ידי הלקוח.

10.4. לתקלות משביתות או תקלות הפוגעות באופן מהותי בשירותים של מכבי שרותי בריאות, כהגדרת מכבי שרותי בריאות, נדרש זמן תגובה של עד 4 שעות בכל שעות היממה, שבעה ימים בשבוע (7*24). יש להציג צוות בישראל שמסוגל להגיע לאתר מכבי בבעיה מסוג זה, לרבות החלפת חומרה תקולה באתר בלקוח.

10.5. על הספק להחזיק מלאי המיועד באופן בלעדי למקרים בהם תידרש החלפה של הציוד, עקב תקלה משביתה (או כזו הפוגעת באופן מהותי בשירות המסופק ע"י המוצר), אשר לא ניתן לפתור באופן מיידי (בכפוף ל-SLA). יש להציג מסמכי זיהוי (מספר סידורי והוכחת רכישה) של ההתקן החלופי.

## 11. דרישת מספק הפתרון:

11.1. על הספק להיות בעל הסמכה של יצרן המערכת להתקנה, הטמעה ותחזוקה של הפתרון כולל רכיבי ה-HSM .

11.2. על הספק להוכיח קיום קשרי עבודה עם יצרן המערכת (פתיחת תקלות, יכולת שינויים, עדכונים וכד').

11.3. על הספק להיות בעל ניסיון בהתקנה של המוצר המוצע, 3 התקנות לפחות בשנתיים האחרונות (תצורה דומה לדרישות מפרט זה) בארגונים גדולים ומורכבים בישראל (1000 משתמשי קצה לפחות) המשרתות סדר גודל דומה של חותמים.
יש להעביר שמות ממליצים ופרטי התקשרות עם ממליצים כאמור.

11.4. יש לציין את כוח האדם המוצע לפרויקט זה ולפרט את ניסיונו בהתקנה ואינטגרציה של מערכת חיתום מרכזית.

11.5. יש לפרט את היערכות הספק להתמודדות עם ה- SLA הנדרש בסעיף 10 כאמור לעיל.

**12. <u>מחיר ותנאי תשלום:</u>**

12.1. ההצעה בש"ח או בדולר ארה"ב.

12.2. המחירים אינם כוללים מע"מ.

12.3. תנאי התשלום הינם שוטף + 65 מיום הוצאת החשבונית.

12.4. תוקף ההצעה- 90 ימים.

## 13. טופס ההצעה להקמת מערכת חיתום מרכזית (מהווה את נספח א' להסכם):

התאגיד המציע: _____

יצרן: _____

לקוחות קיימים למוצר /שרות – למתן המלצות:

| חברה | ותק במכירת המוצר /שרות | איש קשר | טלפון |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

13.1. מערכת החיתום:

| | פריט | כמות | מחיר יחידה | מחיר כולל | מטבע |
|---|---|---|---|---|---|
| 13.1.1. | עלות מערכת חיתום מרכזית עבור סביבת הייצור, | 1 | | | |
| 13.1.2. | מכונת מערכת חיתום מרכזית נוספת למימוש HA | 1 | | | |
| 13.1.3. | רכיב שלישי כגיבוי בענן (מיקום הענן ותצורת ה appliance ) – CLUSTER/ עבודה במקרה כשל פניה לשירות הענני להמשך תפעולי. עלות שירות ושימוש לשנה | 1 | | | |
| 13.1.4. | עלות פיתוח ממשק זיהוי באמצעות OTP אפליקצית Vasco DigiPass , SMS ו- Token (כמתואר בסעיף 6.2) | 1 | | | |
| 13.1.5. | עלות פיתוח ספריית תוכנה (DLL) לחיתום ובדיקת חיתום שיהווה ממשק לקליקס כמתואר בסעיף 6.2 | 1 | | | |
| 13.1.6. | התקנה, אינטגרציה, הפעלה, הטמעה, הדרכה, רישוי, ותמיכה במערכת כאמור בסעיפי הבקשה. כולל אחריות ותחזוקה לשנה בתנאי SLA כמפורט בבקשה סעיפים 6.1 ו- 6.3 עד 6.12 | 2 | | | |
| 13.1.7. | רישיון בודד לחותם | 8000 | | | |

| | | | | | |
|---|---|---|---|---|---|
| 13.1.8. | עלות הרחבת רישוי לחותם (עלות יחידה) | 1 | | | |

13.2. תחזוקת מערכת החיתום:

| | פריט | כמות | מחיר לשנה | מחיר כולל | מטבע |
|---|---|---|---|---|---|
| 13.2.1. | עלות אחריות ותחזוקה שנתית למערכת חיתום מרכזית בסביבת הייצור (כלל הרכיבים – מקומיים וענן), בתום תקופת אחריות והתחזוקה הראשונית, עפ"י המפורט בתנאי SLA כמפורט בבקשה סעיפים 9 עד 10.<br>כולל כל הפיתוחים וההתאמות שבוצעו ורישיונות המשתמשים כמפורט בסעיף 13.1 | 1 | | | |
| 13.2.2. | **<u>אופציה</u>**: <u>אחריות ותחזוקה</u>, בתנאי ה- SLA כמפורט בבקשה,<br>בהזמנה מראש ל- 3 שנים. יודגש כי התשלום בגין תחזוקה לשנה שניה ושלישית יבוצע בשנת מתן השירות הקלנדרית (כלומר תשלום תחזוקה בגין 2024 ישולם ב- 2024).<br>**<u>(לכלל מרכיבי מערכת החיתום)</u>** | 3 | | | |

## 14. <u>טופס ההצעה להקמת תשתית HSM</u>

14.1. סך מרכיבי עלות עבודת הקמה, הטמעה והדרכה:

| | פריט | זמן (שעות) | עלות לשעה |
|---|---|---|---|
| 14.1.1. | הקמה ואינטגרציה של המערכות (עפ"י הנדרש בפרק 7. באחריות הספק לבצע יישום מלא של כל הפתרון מקצה לקצה לרבות אספקת כל הרכיבים הנדרשים ליישום מלא של הפרויקט כגון אפליקציות נדרשות (למעט ה-CA של מיקרוסופט ושרתים), כל המודולים וכל הדרישות. | | |
| 14.1.2. | הדרכה (בהתאם לדרישה 7.3,7.7) | | |
| 14.1.3. | תיעוד (בהתאם לדרישה בסעיף 7.2,7.7,7.8) | | |
| 14.1.4. | כתיבת נהלים (בהתאם לדרישה בסעיף 6.12) | | |

14.2. אופציה: עלויות Professional Services לעבודות נוספות מעבר לתכולת הבקשה

| | פריט | זמן | עלות לשעה |
|---|---|---|---|
| 14.2.1. | מהנדס מערכת בכיר | 1 שעה | |
| 14.2.2. | מתכנת – לכתיבת ממשקים חדשים בין מערכות מכבי למערכת החיתום המוצעת מעבר לנדרש בתכולה הבקשה | 1 שעה | |
| 14.2.3. | עלות שעת עבודה PROFESSIONAL SERVICES להוספת שירותים , התקנות HSM / CA/ מערכת חיתום, תפעול שוטף של המערכות וכד' מעבר לנדרש בתכולה הבקשה | 1 שעה | |

14.3. עלות מימוש של חתימות מאובטחות במודל SaaS, כולל כל הנדרש עפ"י בקשה זו, בפרט לעמידה בנוהל 107

| | פריט | כמות | מחיר | מטבע |
|---|---|---|---|---|
| 14.3.1. | עלות חתימה מאובטחת | 8000 | | |

## 1. מונחים רלוונטיים לתקן CEN/prEN 419241-1:2014 E

1.1. **AdES** Advanced Electronic Signature or Advanced Electronic Seal

1.2. **CC** Common Criteria, ISO/IEC 15408, Evaluation criteria for IT security

1.3. **CEN** Comité Européen de Normalisation (European Committee for Standardization)

1.4. **CEN/ISSS** CEN Information Society Standardization System

1.5. **HSM** Hardware Security Module

1.6. **ISO/IEC** International Organization for Standardization / International Electrotechnical Commission

1.7. **ISSS** Information Society Standardization System

1.8. **LoA** Level of Assurance

1.9. **PIN** Personal Identification Number

1.10. **QC** Qualified Certificate (for electronic signature or for electronic seal)

1.11. **QES** Qualified Electronic Signature or Qualified Electronic Seal

1.12. **QSCD** Qualified (electronic) Signature Creation Device or Seal Creation Device

1.13. **rSCDev** Remote (electronic) Signature Creation Device or Seal Creation Device

1.14. **SAD** Signer's Activation Data

1.15. **SCA** Signature Creation Application or Seal Creation Application

1.16. **SCC** Sole Control Component

1.17. **SCD** (electronic) Signature Creation Data or Seal Creation Data

1.18. **SCDev** (electronic) Signature Creation Device or Seal Creation Device

1.19. **SCDid** SCD Identifier

1.20. **SD** Signers' Document

1.21. **SDO** Signed Data Object

1.22. SGSP Signature Generation Service Provider or Seal Generation Service Provider

1.23. **TSCM** Trustworthy Signature Creation Module or Trustworthy Seal Creation Module

1.24. **TSP** Trust Service Provider

1.25. **TW4S** Trustworthy System Supporting Server Signing

תאריך: _____

# הסכם

בין מכבי שרותי בריאות, להלן מכבי לבין _____ח.פ. _____ (להלן- "**הספק**") לרכישה, יישום והטמעת מערכת חיתום דיגיטלי ושמירת מפתחות (HSM) בתצורה היברידית (להלן– "**המוצרים והשירותים**").

## 1. תקופת ההסכם

1.1 הסכם זה יעמוד בתוקף למשך שנה החל מיום _____ ועד יום _____(להלן: "**תקופת ההסכם**").

1.2 על אף האמור לעיל, מכבי תהא רשאית להביא הסכם זה לידי סיום, בכל שלב ומכל סיבה שהיא, וזאת על-ידי משלוח הודעה בכתב 30 יום מראש. במקרה זה תשלם מכבי לחברה את הסכומים שהתחייבה לשלם עד למועד שבו הופסקה ההתקשרות, או החברה תחזיר למכבי את הסכומים ששולמו עבור התקופה שלאחר מועד הפסקת ההתקשרות.

## 2. תמורה

2.1 רשימת המוצרים והשירותים המסופקים על ידי החברה למכבי ומחיריהם יהיו כמפורט בהצעת הספק המצ"ב **כנספח א'** להסכם זה.

2.2 היה והספק יזכה בבקשה של החשב הכללי לאספקת נשוא ההסכם במהלך תקופת ההתקשרות עם מכבי , תעמוד למכבי הזכות, על פי שיקול דעתה הבלעדי, להתקשר עם הספק הזוכה, על בסיס המחירים בהם זכה בחשב הכללי, מתחילת התקשרותו עם החשב הכללי ועד סיום ההתקשרות עם החשב הכללי.

## 3. תנאי תשלום

3.1 התמורה תשולם כנגד חשבונית מס בתנאי תשלום של שוטף + 65 יום מיום הוצאת החשבונית ואישור קבלת המערכת ע"י מנהל מחלקת תשתיות מחשוב במכבי. החשבונית תוגש לא יאוחר מ-10 (עשרה) ימים מתום חודש הפעילות. אם תוגש לאחר מועד זה, התשלום ידחה למועד התשלום הבא.

3.2 הספק יציג בפני מכבי אישור עפ"י חוק עסקאות גופים צבורים (אכיפת ניהול חשבונות) תשל"ו – 1976 המעיד על ניהול פנקסי חשבונות עפ"י פקודת מס הכנסה וחוק מע"מ או פטור מניהול זה, על כי הוא נוהג לדווח לפקיד השומה על הכנסותיו וכן נוהג לדווח על עסקאותיו למע"מ בהתאם לחוק.

## 4. שרותי תמיכה ואחזקה

4.1 שירותי התמיכה והתחזוקה יינתנו בשרות טלפוני ו/או באמצעות תקשורת מחשבים ו/או באתר מכבי, בהתאם לאופי הפניה ותוך הפעלת שיקול דעת מקצועי של הספק בשיתוף מכבי, ויכללו טיפול תמיכה ופתרון תקלות, טיפול בבאגים, אספקה והתקנה של גרסאות ומהדורות חדשות של התוכנה, ללא תשלום נוסף.

4.2 שירותי התחזוקה יינתנו בימים א' עד ה', בשעות העבודה בזמן ישראל. (להלן – "**שעות העבודה**"), הספק יעמיד מוקד טלפוני מאויש לקבלת קריאות שרות משך שעות העבודה.

4.2.1 זמני התגובה לקריאות שירות הינו עד יום עבודה אחד, לכל היותר NBD

4.2.2 שירות התחזוקה כולל עבודה רצופה עד לתיקון מלא של התקלה. הספק יעשה כמיטב יכולתו כדי לתקן את התקלה במהירות האפשרית, ובמידת הצורך, יספק פתרונות ביניים עד לתיקון התקלה באופן סופי ומוחלט.

4.2.3 במקרה של כשל המפריע לתפקוד שוטף של מערכות בארגון, יתבצעו פעולות מיידיות ורצופות להשבת המערכת לתפקוד מלא ותקין.
במידה והבעיה לא נפתרת תהיה אפשרות לנציג מכבי להעלות את רמת החומרה

4.2.4 לתקלות משביתות או תקלות הפוגעות באופן מהותי בשירותים של מכבי שרותי בריאות, כהגדרת מכבי שרותי בריאות, נדרש זמן תגובה של 4 שעות בכל שעות היממה, שבעה ימים בשבוע (7*24).

## 5. זכויות קנין רוחני

5.1 הספק מצהיר כי הוא בעל הזכויות לשיווק ו/או הפצת המוצרים והשירותים וכי אין כל מניעה חוקית או אחרת המונעת ממנו לספק בכל דרך את המוצרים והשירותים למכבי וכי אין באספקת המוצרים והשירותים משום הפרת פטנט ו/או פגיעה כלשהי בזכויות של חברה ו/או גוף לרבות אדם אחר כלשהו.

5.2 היה ותתבע מכבי על-ידי גורם כלשהו בגין הפרת זכויות וטענות של צד שלישי במוצרים, מתחייב הספק לשפות לאלתר את מכבי בגין כל הוצאה שתיגרם לחברה כתוצאה מתביעה שכזו.

## 6. מועסקי הספק

6.1 הספק מצהיר בזה, כי כל האנשים שיועסקו על ידו לצורך אספקת המוצרים והשירותים למכבי ייחשבו לכל צורך כעובדיו או שלוחיו ולא יחשבו כעובדיה או שלוחיה של מכבי, במישרין או בעקיפין, ויועסקו על ידו באופן בלעדי, על חשבונו הוא בלבד, ועליו תחול האחריות לגבי תביעותיהם הנובעות מיחסיו עימם.

6.2 הספק יהא אחראי כלפי עובדיו, שליחיו וכל מי שפועל מטעמו בגין מוות, נזק גופני, או נזק לרכוש שייגרם להם, בין במישרין ובין בעקיפין, כתוצאה מתאונה או מנזק שאירע בעת אספקת המוצרים ו/או מתן שרות למכבי.

6.3 הספק מתחייב לפצות ו/או לשפות את מכבי, בגין כל נזק ו/או הוצאה שיגרמו לה, אם יקבע על ידי רשות מוסמכת, כי המצב המשפטי ו/או העובדתי שונים מהמוצהר בהוראות פרק זה.

**7. <u>אנשי קשר</u>**

7.1 מכבי ממנה בזאת את חן וולף להיות איש הקשר הישיר עם הספק.

7.2 הספק ממנה בזאת את _____ להיות איש הקשר הישיר עם מכבי.

**8. <u>הסבת הסכם</u>**

הספק איננו רשאי למסור, או להעביר לאחר, את זכויותיו על פי ההסכם, או את החובות הנובעות ממנו, אלא בכפוף לאישור מראש ובכתב של מכבי.

**9. <u>אחריות</u>**

9.1 הספק יהא אחראי על פי דין לכל נזק ו/או אובדן ו/או פגיעה ו/או הפסד, לגוף ו/או לרכוש שיגרמו למכבי ו/או למי מטעמה ו/או למבוטחיה ו/או לצד שלישי כלשהו עקב ו/או בקשר עם ייצור ו/או אספקת המוצרים ו/או מתן השירותים, כמפורט ומוגדר בהסכם זה.

9.2 הספק מתחייב לפצות ו/או לשפות את מכבי ו/או מי מטעמה, מיד עם דרישתה הראשונה של מי מהן, בגין כל נזק ו/או הוצאה, (לרבות הוצאות ושכ"ט עו"ד בגין תביעה שתוגש כנגד מי מהם), שייגרמו להן כתוצאה מאירוע שהינו באחריותו של הספק ו/או מי מטעמו ו/או בשמו, על פי הסכם זה או על פי כל דין.

**10. <u>סודיות</u>**

הצדדים מתחייבים לשמור בסודיות את ההסכם ולא להעביר את ההסכם ו/או תוכנו לכל צד שלישי. התחייבות זאת תהא בתוקף גם לאחר סיומו של ההסכם מכל סיבה שהיא.

**11. <u>אבטחת מידע</u>**

11.1 **<u>כללי</u>**

11.1.1 הספק יגדיר איש קשר אחראי לאבטחת המידע שבאחריותו לוודא את יישומן של הדרישות שיובאו להלן.

11.1.2 הספק מתחייב כי הנו בעל הסמכה לתקן בינלאומי לניהול אבטחת מידע – ISO27001 או לתקן לאבטחת מערכות מידע במוסדות בריאות ISO27799. הספק מתחייב להעביר צילום/סריקה של תעודת הסמכה בתוקף במסגרת חתימת ההסכם.

11.1.3 לספק יהיו נהלי אבטחת מידע מעודכנים וזמינים לעובדי הספק. מכבי רשאית לבקש מהספק בכל עת עותק מנהלים אלו.

11.1.4 במקרים שבהם הספק מקבל ממכבי מידע המכיל פרטים אודות חברי מכבי ו/ואו עובדיה, הספק מצהיר כי הוא פועל כנדרש על פי חוק הגנת הפרטיות התשמ"א-1981, התקנות מכוחו והנחיות הרשות להגנת הפרטיות במשרד המשפטים (להלן ביחד: "החוק"), וכי הוא נוקט באמצעי אבטחה ובקרה כמתחייב מהחוק.

11.1.5 במידה והספק נדרש לאחסן מידע רגיש אודות חברי מכבי ו\או עובדי מכבי הספק נדרש לרשום את מאגר המידע במשרד או להצהיר על שימוש במאגר מידע קיים כמתחייב מהחוק.

11.2 אבטחת מידע לוגית במקרה שבמהלך מתן השירותים למכבי הספק או מי מטעמו יחזיק מידע של מכבי על אמצעי מחשוב נייח או נייד שאינו ברשת המחשוב של מכבי, אזי יפעל הספק כאמור בסעיפים שלהלן:

11.2.1 <u>הגדרות</u>

11.2.1.1 מידע חסוי - מידע עסקי/ מידע רפואי/ מידע על עובדי מכבי

11.2.1.2 מידע חסוי ביותר - מידע מזוהה ופרטני בנושאים הבאים: איידס, פסיכיאטריה, התמכרויות וסמים, הפסקות הריון, בדיקות גנטיות ונתונים גנטיים, בדיקות קשרי משפחה, תרומות זרע, תרומות ביציות, טיפולי פוריות, אימוץ, מקרי אונס או תקיפה מינית, מחלות מין ואלימות במשפחה

11.2.2 במידה והספק מעבד מידע עבור מכבי המסווג כ"חסוי או חסוי ביותר" ע"פ מדיניות סיווג המידע של מכבי, השרתים או המחשבים המכילים מידע של מכבי לא יחוברו באופן ישיר לרשת האינטרנט ולרשתות חיצוניות (בחיוג או בנל"ן). חריגה מתנאי זה מחייבת אישור מראש של מנהל אבטחת המידע והגנת הסייבר של מכבי . למען הסר ספק מאושר לחבר את השרתים או המחשבים לרשת האינטרנט כאשר מיושמות מערכות הגנה בניהם (כגון FW וכדומה).

11.2.3 הספק יישם מידור פנימי בגישה לקבצים המכילים מידע של מכבי. הגישה לקבצים אלה תתאפשר רק למי שעבודתם ותפקידם אצל הספק מחייבים זאת, ולמי שחתמו על התחייבות לשמירת סודיות מול מכבי.

11.2.4 הספק יוודא הצפנה של קבצים המכילים מידע של מכבי המסווג כ"חסוי או חסוי ביותר" ע"פ מדיניות סיווג המידע של מכבי.

11.2.5 קבצים המכילים מידע של מכבי המסווג כ"חסוי או חסוי ביותר" ע"פ מדיניות סיווג המידע של מכבי יועברו מהספק אל מכבי באופן מוצפן.

11.2.6 אין להעביר קבצים המכילים מידע של מכבי בדוא"ל ו/או בכל אמצעי תקשורת אחר לגורמים אחרים ללא אישור בכתב ממכבי.

11.2.7 בתחנות העבודה של הספק תשמר אבטחת המידע באופן הבא:

11.2.7.1 לא יישמרו קבצי מכבי על הדיסק הקשיח של התחנה (למעט לגבי חברה או יחיד ללא רשת משתמשים).

11.2.7.2 הכניסה לתחנה תהיה באמצעות USER ID וסיסמא אישית

11.2.7.3 אורך הסיסמא יהיה לפחות שבעה תווים.

11.2.7.4 הסיסמאות יוחלפו כל שלושה חודשים לפחות.

11.2.7.5 משתמש שנכשל בעת ניסיון הזדהות 5 פעמים ברציפות יינעל באופן אוטומטי.

11.2.7.6 נדרשת אכיפה שנועלת את מחשבי הארגון לאחר 20 דקות ללא שימוש במחשב.

11.2.7.7 תותקן תכנת הגנה תקנית ומעודכנת כנגד וירוסים.

11.2.7.8 מערכת ההפעלה המותקנת על תחנות העבודה נדרשות להיות מעודכנת בעדכוני האבטחה האחרונים שהופצו על ידי היצרן.

11.2.8 הוצאת דיסק קשיח משרתי הספק או ממחשבים אישיים (למעט לגבי חברה או יחיד ללא רשת משתמשים) לצורך תיקון או לכל מטרה אחרת כשעליהם נמצאים קבצים המכילים מידע של מכבי אסורה .במקרה כזה יש למחוק את המידע ולפרמט את הדיסק.

11.2.9 מדיה מגנטית או אופטית כנ"ל תאוחסן בתיאום עם מכבי במקום שהגישה אליו תתאפשר למורשי גישה בלבד.

11.2.10 גיבויים יבוצעו בצורה מסודרת וישמרו במקום סגור ונעול עם גישה לאחראי על הגיבויים בלבד. כמו כן על הספק לקיים נוהל שחזור תקופתי לגיבויים.

11.2.11 אין להעביר קלטות עם גיבויים של קבצים המכילים מידע של מכבי לגופים חיצוניים ללא יידוע מראש.

11.2.12 כל מדיה מגנטית או אופטית או דוח המהווים תוצרי עיבוד מנתוני מכבי יאוחסנו בארון נעול וכן יושמדו וייגרסו לאחר השימוש.

11.2.13 הספק מתחייב להודיע מידית למנהל אבטחת המידע והגנת הסייבר במכבי בגין כל חשש לפגיעה, אובדן ו/או חשיפה של קבצים המכילים מידע של מכבי.

11.2.14 במידה וקיים שימוש בטכנולוגיה של רשת אלחוטית (wifi), הרשת תאובטח לכל הפחות ע"י שימוש בהגדרות הבאות:

11.2.14.1 הרשת (ssid) תוגדר במצב מוסתר שאינו גלוי לכל.

11.2.14.2 יבוצע שימוש בפרוטוקול האבטחה WPA 2.

11.2.15 גישה מרוחקת למערכת הספק תבוצע לכל הפחות על בסיס הגדרות האבטחה הבאות:

11.2.15.1 הגדרת הזדהות רב שלבית בעת הגישה לשירות(MFA).

11.2.15.2 יוגדר לוג אירועים מלא על השימוש בשירות.

11.2.15.3 הגישה לשירות והתעבורה יוצפנו על בסיס הסטנדרטים המקובלים בשוק.

11.3 <u>גישה לרשת ולמערכות מכבי:</u>

במקרה ובמהלך מתן השירותים למכבי יוקצה למי מטעם הספק שם משתמש לרשת ולמערכות מכבי הספק אחראי לכך שמשתמש זה יפעל כאמור בסעיפים שלהלן, מכל אתר ומכל מחשב ממנו יתחבר לרשת מכבי:

11.3.1 לעובד הספק יוגדרו במסגרת תפקידו במכבי משתמש וסיסמא שישמשו לטובת אימות פרטי הזיהוי אל מול מערכות המידע - הסיסמא הינה אישית וסודית. אין להעביר את הסיסמא לאיש, כולל עובדי הספק. אם יימסרו לידי עובד סיסמא ושם משתמש שאינם שלו, חל איסור מוחלט להשתמש בהם.

11.3.2 אין לרשום את הסיסמא במקום גלוי. במידת הצורך יש לבצע שימוש במקום אחסון מאובטח - אחסון בכספת פיזית לנייר ושימוש בהצפנה לקובץ מחשב.

11.3.3 על עובד הספק הנעדר מעמדת העבודה להקפיד לנעול את העמדה.

11.3.4 אין לחבר לעמדת העבודה התקנים חיצוניים כגון כונני USB, מודמים, נגני מדיה וכדומה, וכן כל אמצעי אחר העושה שימוש בתווך תקשורת אלחוטי (Bluetooth, Wireless, Infrared) ועוד .

11.3.5 אין לבצע כל שינוי בעמדת העבודה באורח עצמאי על ידי העובד, כולל התקנת תוכנות.

11.3.6 אין לשמור קבצים באופן מקומי על עמדת העבודה. הקבצים יישמרו על כונני הרשת הפנימית במקומות ייעודיים ע"פ רמת הסיווג שלהם.

11.3.7 באם עובד הספק חושד כי נעשה שימוש לא מורשה בעמדת עבודתו, עליו לדווח מידית למחלקת אבטחת מידע והגנת הסייבר במכבי.

11.4 שימוש באמצעי mobile ומחשבים ניידים:

במקרה שבמהלך מתן השירותים למכבי יוחזק מידע של מכבי באמצעי מחשוב ניידים (לדוגמא: DOK, Laptop, Mobile Phone, Tablet), מחויב עובד הספק לפעול כדלקמן:

11.4.1 אמצעי ה-mobile יימצא בהשגחת עובד הספק בכל עת. במידה והעובד אינו לוקח את אמצעי המחשוב הנייד עמו מסיבה כלשהי, עליו לנעול אותו במקום בטוח.

11.4.2 אם אמצעי ה-mobile אבד, על העובד או איש הקשר מטעם הספק לדווח מידית למנהל אבטחת המידע והגנת הסייבר ו/או לקב"ט ולפרט את סוג המידע של מכבי שהיה על אמצעי המחשוב שאבד וכיצד הוא מוגן ומגובה.

11.4.3 במידה וייעשה שימוש בקבצים המכילים מידע על לקוחות מכבי ו/או עסקי מכבי ו/או נתונים על מערכות מכבי – על הספק לוודא כי מסמכים אלה יוצפנו פרטנית ו/או יוצפן כל התקן זיכרון.

11.4.4 ככלל, לא יוצאו התקני זיכרון מאמצעי המחשוב הנייד לתיקון או לכל מטרה אחרת כשעליהם נמצאים קבצים המכילים מידע של מכבי .במקרה שתבוצע פעולה כזו, על המשתמש למחוק את המידע ולפרמט את הדיסק.

11.4.5 אין להעביר אמצעי גיבוי של קבצים המכילים מידע של מכבי לגופים חיצוניים ללא אישור מראש ובכתב ממנהל אבטחת המידע והגנת הסייבר במכבי.

11.5 **<u>ארכיטקטורה</u>**

11.5.1 האתרים יהיו תחת Domain מכבי (כלומר הURL של האתרים יהיו בDomain מכבי).

11.5.2 חל איסור עקב מגבלות טכנולוגיות לעבוד עם שירותים המבוססים על פרוטוקול Web socket. במידת הצורך ניתן לפנות לאבטחת מידע והגנת הסייבר במכבי על מנת לאפיין פתרון חלופי.

11.5.3 שליחת ה- SMS/ WhatsApp תבוצע אך ורק למספרי הטלפון המעודכנים במכבי. זהות השולח תהיה מכבי שירותי בריאות.

11.5.4 שליחת המיילים יועברו מכתובת של מכבי בלבד. לצורך כך הספק מתחייב להעביר כתובות IP למכבי לצורך הגדרת SPF.

11.5.5 ממשק הניהול– יוגבל ברמת תקשורת לכניסה רק ממחשבי מכבי, ומחשבי הספק (לצורכי תמיכה).

11.5.6 הספק יישם את הגדרות האבטחה הבאות:

11.5.6.1 האתרים המשמשים את הפתרון ימוגנו על ידי Web application firewall של מכבי שירותי בריאות.

11.5.6.2 ממשק ניהול (מכל סוג) לא יהיה נגיש לכל כתובות האינטרנט, אלא יפתח ב FW רק לכתובות ספציפיות של מכבי ושל הספק.

11.5.6.3 כל הנתונים ישמרו מחוץ לשרת ה WEB בשרת מסד הנתונים ייעודי באיזור ממודר ברשת.

11.5.6.4 שרת מסד הנתונים ישב בסגמנט ייעודי מופרד ב FW מסגמנט שרת ה WEB . סיגמנט זה יהיה חסום לגישה אל ומ– האינטרנט.

11.5.6.5 עובדי מכבי יזדהו למערכת ע"י הזדהות מול IDP של מכבי (מימוש יתבצע ע"י SAMEL).

11.5.6.6 תבוצע הפרדה בין שרתי מכבי לשרתי הספק ושרתי לקוחות נוספים. ההפרדה תבוצע לבאים: שרת זהויות, מסדי נתונים, שרתי WEB ואפליקציה.

11.5.6.7 תבוצע הפרדה בין סביבת הייצור לסביבת הפיתוח והבדיקות. ההפרדה תבוצע הן ברמת אפליקציה והן ברמת תשתיות (שרת וב, שרת מסד נתונים וכו').

11.5.6.8 יוגדרו סיגמנטים ייעודיים עבור שרתי מכבי אשר יופרדו מבחינת תקשורת משאר שרתי הספק (הכוונה למערכות ההפעלה, ולא לברזלים המחזיקים את כלל השרתים הווירטואליים).

11.5.6.9 באתרים יופעלו שירותי\מערכות הבקרה הבאים (השירותים\מערכות יופעלו במוד הגנה אקטיבית (חסימה) ולא במוד למידה).

11.5.6.9.1 FW – אפיון והגדרה של ה WAF באופן אקטיבי על בסיס התאמה לאתר האינטרנט.

11.5.6.9.2 IPS

11.5.6.9.3 ממשק הפלטפורמה ל- WAF של מכבי

11.5.6.9.4 Anti DOS\DDOS (להגנה ספציפית על אתרי מכבי).

11.5.6.9.5 אנטי וירוס - האנטי וירוס יעודכן ברמה יומית.

11.5.6.9.6 עדכוני אבטחה – מערכות ההפעלה המשמשות את השירות יעודכנו באופן שוטף בעדכוני האבטחה הרלוונטיים. עדכון אבטחה ברמת חומרה קריטית – על פי הגדרות היצרן, יותקן עד לרבעון לאחר יציאתו.

11.5.6.9.7 הקשחת שרתים - כל מערכות המידע יעברו הקשחה על פי הסטנדרטים המקובלים בשוק.

11.5.6.10 מועמדים חיצוניים (שאינם עובדי מכבי) יזדהו למערכת באמצעות חשבון אישי באתר.

11.5.6.11 גישה לשירותים מחוץ לרשת מכבי עבור עובדי מכבי תתאפשר רק מרשת מכבי.

## 11.6 <u>ממשקי Web Service</u>:

כל ממשקי הWeb Services ינוהלו ויאובטחו לפי הנחיות מכבי שירותי בריאות ויכללו לכל הפחות:

11.6.1 תצורת TLS עם זיהוי תעודות דו כיווני (הכולל תעודה דיגיטלית ייעודית לשרת, ותעודה שניה ייעודית לצד ה- Client.

11.6.2 גישה לשירות (API) במכבי דורשת פניה באמצעות כתובת IP קבועה בלבד. לא תתאפשר פניה לשירות מכתובת DHCP או כתובת שאינה קבועה.

11.6.3 בכל הממשקים מול מכבי, מכבי תהווה את צד ה- Server בממשק, כאשר הספק הוא ה- Client.

**11.6.4** כל גישת ממשק לשירות תבוצע דרך רכיב API MGMT (APIC, F5 DP וכו) שיבצע הזדהות, מידור ו Schema validation.

**11.6.5** לכל שירות יהיה הזדהות ייחודית והרשאות ייחודיות מול שירותים אחרים.

11.6.6 מכבי תוכל לספק תעודות דיגיטליות לכל הצדדים בתהליך התשתיתיים והאפליקטיביים, הכוללים את תשתיות הרשת (Active Directory לדוגמא), מסדי הנתונים, האפליקציה, וה- WEB.

11.6.7 במידת הצורך יועבר פירוט מלא של דרישות הגנה מפני התקפות אפליקטיביות.

11.7 <u>הצפנה</u>

11.7.1 דרישות תעודת הצפנה:

11.7.1.1 תעודת הספק תהיה מ issuer חיצוני ולא CA מקומי

11.7.1.2 אלגוריתם של התעודה תהיה sha256

11.7.1.3 התעודה תכיל CRL Distribution Points

11.7.2 דרישות לגבי ההצפנה:

11.7.2.1 העבודה מול הספק תהיה בתוך TLS ver. 1.2 or above

11.7.2.2 התקשורת והמידע יהיו חתומים\מוצפנים ע"י התעודות. ( כולל ה response מהספק)

11.8 <u>ניטור אירועים</u>

11.8.1 יוגדר ויופעל לוג אירועים מלא על כלל האירועים בכלל מרכיבי המערכת.

11.8.2 לוג האירועים יוגדר על הבאים:

11.8.2.1 בכל מודול ומערכת שמאחסנת מידע של מכבי.

11.8.2.2 בכל רכיב בשרת: מערכת הפעלה, מסד הנתונים, והGUI.

11.8.2.3 בכל רכיב במערכת: אתר משתמשים, backoffice וכו'.

11.8.3 לוג אירועים יופעל על האירועים הבאים:

11.8.3.1 כניסות למערכת – מוצלחות או כישלונות.

11.8.3.2 כל גישה לנתונים, כולל קריאה בלבד.

11.8.3.3 כל גישה ללוג האירועים, שינוי הגדרות בו או מחיקתו.

11.8.3.4 כל פעולה המבוצעת על ידי משתמש ניהול המערכת \ שרת.

11.8.3.5 שינוי הגדרות מערכת. כולל שינוי במערכת המשתמשים וההרשאות.

11.8.4 רישום כל אירוע יכלול את הערכים הבאים:

11.8.4.1 מועד ביצוע הפעולה.

11.8.4.2 שם משתמש מבצע הפעולה.

11.8.4.3 כתובת מקור.

11.8.4.4 סוג ה – Client.

11.8.4.5 שם הפעולה.

11.8.4.6 סטטוס – הצלחה\כישלון.

11.8.4.7 תיאור הפעולה.

11.9 **<u>פיתוח מאובטח</u>**

במקרה שפיתוח האתרים יבוצע על ידי הספק, ייושמו דרישות הפיתוח הבאות:

11.9.1 האתר יפותח בסטנדרט פיתוח מאובטח – OWASP-Top 10

11.10 אפליקציות ותשתיות המערכת מחויבות להיות מוקשחות בהתאם לסטנדרטים המקובלים בשוק.

11.11 במידה והספק מפתח ברשת מכבי, יש לפעול בהתאם לנהלים הבאים:

11.11.1לעבוד עם הכלים הקיימים ברשת מכבי.

11.11.2לעבוד בתשתיות ה DevOps הקיימות של מכבי.

11.11.3להורדת כלים נוספים יש לקבל אישור אבטחת מידע.

11.11.4 סביבות הפיתוח המשמשות לטובת מכבי שירותי בריאות להיות מפורדות מסביבות של לקוחות אחרים.

11.11.5 סביבות הפיתוח לא יהיו נגישות בשום אופן לרשת האינטרנט.

11.12 גישה לסביבות הפיתוח יהיו נגישות אך ורק לכתובות IP של מכבי.

11.12.1 כל שינוי במערכת מחויב לעבור תהליך ניהול שינויים והעלאה לייצור שיכלול שלב פיתוח, שלב QA ושלב עליה לייצור.

11.12.2 כל תהליך שינוי במערכת הכולל שינוי בקוד מחויב לעבור תהליך של Code Review לצורך מזעור סיכוני אבטחת מידע כתוצאה מטעויות בקוד.

11.12.3 אפליקציות ותשתיות המערכת מחויבות להיות מוקשחות בהתאם לסטנדרטים המקובלים בשוק.

11.12.4 חל איסור לבצע שימוש במידע חסוי/חסוי ביותר/ מידע אישי מזוהה כ Test Data בתהליכי QA ופיתוח. לתהליכים אלו יש להשתמש ב Data אנונימי או ב Data רנדומלי בלבד

11.12.5 חריגה מאופשרת באישור מראש על ידי מכבי שירותי בריאות.

11.13 יש לבצע מבדקי חדירות לפני עלייה לאוויר:

11.13.1 יוגדרו לבדיקה משתמשים וסביבה לביצוע הבדיקה.

11.13.2 לאחר הבדיקה יפורסם דוח ממצאים.

11.13.3 לאחר ישיבת תיקוף יש לטפל בממצאים ברמה גבוהה ובינונית.

11.13.4 לאחר הטיפול בממצאים יש לבצע בדיקת חדירות חוזרת.

11.13.5 העלייה לאוויר מאושרת לאחר שכל הממצאים הגבוהים/בינוניים טופלו.

11.14 **<u>אבטחת מידע בענן:</u>**

במקרה שבמהלך מתן השירותים למכבי יוחזק מידע של מכבי בשירותי ענן, מחויב הספק לפעול כדלקמן:

11.14.1 ההתקשרות תאושר רק לאחר אישור "ועדת ענן ארגונית" של מכבי.

11.14.2 ספק הענן יהיה ב- EU Region בלבד

11.14.3 ספק שירותי הענן יגדיר איש קשר לנושאי אבטחת מידע(בקרות ואירועים).

11.14.4 ספק שירותי ידווח על כל חשש או אירוע מהותי בנושא אבטחת מידע וסייבר.

11.14.5 ספק הענן יודיע לארגון – ודרכו גם למכבי - על כל דרישה של הרשויות למסירה/עיון במידע של מכבי או לקוחותיה.

11.14.6 ספק הענן יודיע לארגון על כל שינוי בבעלות הספק, ויבטיח כי כל שינוי כאמור יבוצע רק בכפוף לקיום התחייבויות הבעלים החדשים כלפי הארגון, על פי חוזה ההתקשרות שנחתם עם הספק.

11.14.7 העברת מידע לשירות הענן תבוצע לאחר חתימת הספק על הסכם סודיות.

11.14.8 מכבי רשאית לבצע ביקורות ומבדקי חדירה לשירות הענן. כולל ביצוע ע"פ העניין של ביקורת פיזית באתר הספק ע"י נציגי אבטחת מידע ויחידת הביטחון של מכבי. במידת הצורך הספק יוכל לבחור בספק צד ג' המוסכם על מכבי לביצוע הבדיקות מטעמו. דוח הבדיקה במקרה זה יועבר למכבי.

11.14.9 הספק מתחייב להודיע למנהל אבטחת המידע ב- מכבי על כל פעילות של העברת מידע של מכבי ומבוטחיה לשירותי ענן.

11.14.10 על שירות הענן לעמוד בכללי הרגולציה והתקינות הרלוונטיות למכבי על פי צורך והמידע הפעיל בשירות מועבר, מועבד או מאוחסן: , PCI ,ISO-27017, ISO-27001, ISO 27799חוק הגנת הפרטיות.

11.14.11 <u>ניהול זהויות והרשאות בענן:</u>

11.14.11.1 גישה לשירות (הן ניהולית והן מצד לקוח) תבצע במשתמש אישי בלבד.

11.14.11.2 בשירות יוגדר פרופיל ההזדהות בהתאם למדיניות הארגון (חוזק סיסמה, נעילה לאחר כניסות שגויות, ניתוק לאחר אי שימוש וכו').

11.14.11.3 ההזדהות תבוצע באמצעות SAML בלבד. על הספק לחסום כל אפשרויות הזדהויות אחרות.

11.14.11.4 גישת משתמשים תעבור דרך מערכת Proxy של מכבי.

11.14.11.5 ההזדהות תתאפשר מכתובות IP של מכבי בלבד.

11.14.12 <u>אחסון מידע</u>

11.14.12.1 נתוני מכבי ימחקו מהתקני המחשוב בהם משתמש הספק לאחר סיום השימוש בהם או בתום השירות, הראשון מבניהם.

11.14.12.2 על פי צורך, תתאפשר לארגון יכולת למחיקה מוחלטת של המידע מהשירות.

11.14.13 <u>הצפנת המידע</u>

11.14.13.1 נתונים המוגדרים כרגישים (ובכל מקרה במידע רפואי של לקוחות) יוצפנו באחסון.

11.14.13.2 ההצפנה תבוצע בהתאם לסטנדרטים המקובלים בשוק.

11.14.13.3 מפתחות ההצפנה יישמרו באופן בלעדי בידי הארגון במידת האפשר.

11.14.14 <u>ניטור אירועים</u>

11.14.14.1 ניטור אירועים על פי המוגדר בסעיף ניטור אירועים

11.14.15 <u>העברת מידע</u>

11.14.15.1 העברת המידע תבוצע בתווך מזוהה ומוצפן.

11.14.16

11.14.17 הספק מתחייב להחתים את עובדי ושלוחיו הרלוונטיים על הצהרות סודיות, הכוללות, בין היתר, התחייבות לשמירה מוחלטת על סודיות המידע של מכבי. למען הסר ספק, ניתן לבצע שימוש בנוסח ההתחייבות לשמירת סודיות המקובל אצל הספק.

11.14.18 כל מידע המגיע לידי הספק ומי מטעמו יישמר ולא ייעשה בו שימוש שלא לצורך הפעילות מול מכבי.

11.14.19 כל מידע שייחשף במסגרת מתן השירותים הנוגע למכבי ו/או לחבריה ו/או לעובדיה לא יועבר לצד ג' ללא אישור בכתב ממנהל אבטחת המידע והגנת הסייבר במכבי.

11.14.20 הספק מתחייב כי כל ספקי המשנה שלו עומדים בכל דרישות אבטחת המידע במסמך זה.

11.14.21 יש לדווח למנהל אבטחת המידע והגנת הסייבר במכבי בכל חשד לאירוע אבטחת מידע בעל השפעה על המידע של מכבי. במצב של אירוע אבטחת מידע מהותי שנגרם על ידי הספק, הספק יממן את הוצאות הטיפול באירוע.

11.14.22 אין בהתחייבות הספק במסמך זה כדי לגרוע או להפחית מאחריותו של כל עובד שלו לגבי דרישות מסמך זה ו/או לאחריות הספק למילוי הוראותיו ע"י כל עובדיו ושלוחיו.

11.15 הספק אחראי להתאים את רמת אבטחת המידע שלו לסטנדרטים המקובלים בשוק.

11.16 **קנסות**

| הנושא | דרישה | חריגה | קנס |
|---|---|---|---|
| הגנת הפרטיות והסייבר | הסמכה לתקן בינלאומי לאבטחת מידע ISO27001 – או לתקן לאבטחת מידע במוסדות בריאות ISO27799.<br><br>הסמכה חוזרת נדרשת אחת לשנה. בכל שנה. 12 חודשים לאחר העברת האסמכתא הקודמת להנחיה. | אי המצאת תעודת הסמכה לאחד מהתקנים שצוינו | 4% מעלות ההזמנה או 80,000 ₪ הגבוה מבניהם. |

## 12. <u>שונות</u>

12.1 לכל התאגידים/חברות בקבוצת מכבי, לרבות, אך לא רק: אסותא מרכזיים רפואיים בע"מ, בית בלב בע"מ, מכבידנט בע"מ, עמותת קרן מכבי ומכבי טבעי, מכבי אחזקות בע"מ, אגודת מכבי מגן, מכבי יזמות וכד' תהא שמורה הזכות לרכוש את המוצרים מהספק על פי המחירים, ושאר תנאי ההסכם הקבועים בהסכם זה.

12.2 הצדדים להסכם מסכימים בזה, כי למכבי תהיה זכות לקזז כל חיוב כספי שהספק עשוי להיות חב לה מתוך העסקה נשוא ההסכם או מעסקה אחרת, מכל סכום שיגיע לספק ממכבי.

12.3 הספק מצהיר בזה, כי הוא מסכים לכך שההרשאה שניתנה לו על ידי מכבי לספק את הציוד / שרות אינה הרשאה בלעדית, וכי מכבי תהא רשאית, בכל עת, להתיר גם לאחרים להפעיל ולקיים שירות דומה ו/או מקביל עבור מכבי.

12.4 כתובות הצדדים הן כמפורט להלן. כל הודעה בקשר להסכם זה שתשלח בדואר רשום על ידי צד למשנהו על פי הכתובת כמפורט לעיל, תחשב כאילו התקבלה על ידי הצד אליו נשלחה תוך 3 ימים מיום המשלוח, ובמקרה בו נמסרה ביד - בעת המסירה בפועל.

מכבי שירותי בריאות – רח' המרד 27 תל אביב, 68125

הספק _____ - רח' _____

12.5 כתובות הדואר האלקטרוני של הצדדים:

12.5.1 מכבי: wolf_c@mac.org.il

12.5.2 הספק: _____

לראיה באו הצדדים על החתום :

| | |
|---|---|
| _____ | _____ |
| **מכבי שרותי בריאות** | **הספק** |

שם מלא של החותם: _____

חותמת: _____

**<u>אישור</u>**

אני הח"מ, _____, עו"ד, מאשר כי מר/גב' _____, נושא/ת ת.ז. מס' _____, ומר/גב' _____, נושא/ת ת.ז. מס' _____, הינו/ם מוסמכים לחתום על הסכם זה מטעמה של _____, ח.פ./שותפות/עמותה רשומה מס' _____, וכי חתימתו/ם, בצרוף חותמת התאגיד הנ"ל, מחייבת ומזכה את התאגיד הנ"ל לכל דבר ועניין.

_____

_____, עו"ד