מכבי שירותי בריאות
רכש ציוד וחומרים
רחוב המרד 27, תל אביב 6812509

30/03/2026

בקשה לקבלת מידע (RFI)

פיתוח כלי דיגיטלי תומך לגמילה מעישון

(להלן – "הבקשה")

1. כללי

1.1. מכבי שירותי בריאות (להלן –" **מכבי** ") מבקשת לקבל מידע מספקים המסוגלים לספק פתרון דיגיטלי תומך לגמילה מעישון, עבור חברי מכבי, כמפורט במסמך זה ובנספח הדרישות המצורף, (להלן – **"השירותים").**

1.2. מטרת ה- RFI היא למפות פתרונות קיימים, יכולות פיתוח, מודלי התקשרות, הערכת עלות ולוחות זמנים.

1.3. מובהר בזאת כי מטרת הפרסום הינה **קבלת מידע** ואין לראות בכך כל התחייבות מצידה של מכבי לקיים מו"מ או לבחור ספק כלשהו ו/או להתקשר עם מי מהפונים.

1.4. מכבי שומרת לעצמה את הזכות לפרסם פנייה נוספת ו/או לפרסם בקשה להצעות מחיר ו/או לא להתקשר בהסכם כלשהו עם מי מהפונים

1.5. מכבי שומרת לעצמה את הזכות לקיים פגישות הבהרה עם המשיב/ים ו/או לדחות את המענה ללא קיום פגישה, הכל בהתאם לשיקול דעתה הבלעדי.

1.6. לאחר בחינת המידע והתרשמות, מכבי תעשה במידע (כולו או חלקו) זה כראות עיניה, לרבות שימוש לצורך כתיבת מפרטים, מכרז או מסמך דרישות כלשהן ו/או כל שימוש אחר. למוסר המידע לא תהיינה טענות בדבר זכויות יוצרים מכל מין וסוג שהם.

1.7. בקשה זו אינה בבחינת הזמנה להציע הצעות ואינה חלק מהליכי מכרז, לפיכך אין בה כדי ליצור מחויבות כלשהי כלפי איזה מבין המשיבים לה ואין מכבי מחויבת להתקשר עם מי מבין המשיבים כאמור ו/או לפרסם מכרז בנושא. הבקשה נועדה לקבלת מידע בלבד ובעקבותיה תשקול מכבי את המשך פעולותיה בהתאם לשיקולים מקצועיים ועניינים.

1.8. אם יתקיים הליך רכש נוסף בעתיד, תהא מכבי רשאית לשנות או להוסיף תנאים ודרישות מעבר לאשר פורט בבקשה זו – הכול לפי שיקול דעתה המקצועי הבלעדי ובהתאם לצרכיה כפי שיהיו מעת לעת.

1.9. פרסום הבקשה למידע אינו מבטל את זכותה של מכבי להמשך התקשרויות קודמות בהתאם לשיקול דעתה הבלעדי, עם משיב מציע, ואין בעובדה שהמשיב התייחס במסגרת בקשה זו על מנת לבטל ו/או לשנות ו/או לגרוע מזכויות מכבי בהתאם להסכמים קודמים עמו, לרבות מימוש אופציות ככל שהן קיימות.

1.10. את המידע יש למלא על גבי המסמך מצ"ב ו/או ע"ג מסמך של המציע ולשלוח אל **שחר מסר** לדואר אלקטרוני **messer_s@mac.org.il** **<u>עד לתאריך 23.4.2026</u>**

2. רקע

2.1. מכבי שירותי בריאות מעוניינת בפתרון דיגיטלי חדשני המיועד לתמוך בתהליך גמילה מעישון לאורך שלבי ההכנה לקראת הגמילה, ההפסקה והשימור, תוך שימוש בטכנולוגיות מתקדמות מבוססות בינה מלאכותית, לניתוח נתונים והתאמה אישית.

2.2. הפתרון ישמש הן כמסלול עצמאי עבור חברים המעוניינים לנסות להיגמל מעישון ,**על כל סוגיו** , באופן עצמאי, והן ככלי משלים למסלולי גמילה קיימים במכבי כגון: סדנאות, מוקד טלפוני וייעוץ רפואי.

2.3. הפתרון המבוקש יאפשר התאמה אישית של התוכן, ההמלצות והליווי על בסיס נתוני המשתמש, מידע שיוזן על ידי המטופל ומידע שיגיע ממערכות מכבי, וכן יתמוך, ככל שיידרש, בזרימת מידע בין הכלי לבין מערכות מכבי ובקישוריות לכלים ושירותים נוספים של מכבי, והכל בכפוף לאישורי אבטחת מידע, פרטיות וארכיטקטורה של מכבי.

2.4. מכבי מבקשת לקבל מידע מספקים המחזיקים בפתרון קיים, פעיל ומוכח בתחום הגמילה מעישון, או בפתרון קיים בעל התאמה גבוהה לעולם תוכן זה. על הספק לפרט את רמת הבשלות של הפתרון, ניסיונו ביישום בפועל, וההתאמות הנדרשות לצורך הטמעתו במכבי.

3. טבלת התאמה בסיסית לפתרון המוצע

על הספק לסמן ביחס לכל אחת מהדרישות שלהלן האם הפתרון המוצע עומד בדרישה. ככל שהתשובה היא "חלקית" או "לא", יש לפרט בקצרה בהערות.

מס'	דרישת בסיס	כן	חלקית	לא	הערות הספק
3.1	הספק מחזיק בפתרון קיים, פעיל ומיושם בפועל	☐	☐	☐	
3.2	הפתרון מיועד לגמילה מעישון או בעל התאמה גבוהה ומוכחת לעולם תוכן זה	☐	☐	☐	
3.3	לספק ניסיון מוכח ביישום בפועל של פתרון דיגיטלי דומה אצל לקוחות	☐	☐	☐	
3.4	לספק ניסיון מוכח בפיתוח אפליקציות או פלטפורמות מבוססות AI	☐	☐	☐	
3.5	הפתרון כולל תמיכה מלאה בעברית	☐	☐	☐	
3.6	הפתרון כולל יכולות התאמה אישית על בסיס נתוני משתמש, נתוני שימוש ונתונים רלוונטיים נוספים	☐	☐	☐	
3.7	הפתרון כולל יכולות AI או מנגנון דיגיטלי מתקדם לליווי מותאם אישית	☐	☐	☐	
3.8	הפתרון מאפשר, ככל שיידרש, אינטגרציה עם מערכות מכבי ו/או עם התיק הרפואי	☐	☐	☐	
3.9	הפתרון מאפשר איסוף מידע מפעילות המשתמש והעברת מידע נבחר למכבי, כולל יכולות מדידה, דוחות ודשבורדים	☐	☐	☐	
3.10	הפתרון עומד, עקרונית, בדרישות אבטחת מידע, פרטיות והגנת סייבר כמפורט בנספחים	☐	☐	☐	
3.11	הספק מסוגל לספק שירותי תמיכה, תחזוקה והרחבה לאורך זמן	☐	☐	☐	

4. פרטי הספק והמענה הכללי

4.1 פרטי הספק המשיב

יש למלא את הפרטים הבאים:

שם הספק / החברה_____
כתובת : _____
אתר אינטרנט: _____
שם איש קשר: _____
תפקיד: _____
טלפון: _____
דוא"ל: _____

4.2 פרופיל חברה: יש לצרף פרופיל חברה הכולל: שנת הקמה , מבנה בעלות , מספר עובדים, תחומי פעילות עיקריים , פעילות בישראל ובעולם, ניסיון רלוונטי לעולמות בריאות דיגיטלית ,AI ,שינוי התנהגות או ליווי מטופלים, ככל שקיים

פירוט הספק:

5. תיאור טכנולוגי של הפתרון המוצע

5.1 תיאור כללי של הפתרון

יש לתאר את הפתרון המוצע, ובכלל זה:

- סוג הפתרון: מוצר מדף / White-label / התאמה של מוצר קיים / פיתוח ייעודי
- רמת הבשלות של הפתרון
- רכיבים עיקריים
- טכנולוגיות מרכזיות
- רכיבי AI ככל שקיימים
- אופן ההתאמה לצורכי מכבי כפי שהוגדרו במסמך

פירוט הספק:

5.2 ותק הטכנולוגיה בארץ ובעולם: יש לפרט את הוותק של הטכנולוגיה או הפתרון המוצע בישראל ובעולם.

פירוט הספק:

5.3 ניסיון קודם בפרויקטים דומים: יש לפרט ניסיון קודם בפרויקטים דומים, ובכלל זה סוג הפרויקט, תחום הפעילות, היקף היישום ורמת הדמיון לפתרון המבוקש.

פירוט הספק:

5.4 תקנים, הסמכות ואישורים: יש לפרט את התקנים, ההסמכות והאישורים הקיימים ביחס למערכת או לפתרון המוצע.

פירוט הספק:

5.5 מידע טכני נוסף: יש לצרף כל מידע, מפרט, מסמך או חומר טכני נוסף הרלוונטי להבנת הפתרון המוצע.

פירוט הספק:

6. לקוחות מרכזיים ואנשי קשר ממליצים

6.1 לקוחות מרכזיים שבוצע עבורם פרויקט דומה: יש לפרט לקוחות מרכזיים שבוצע עבורם פרויקט דומה לפתרון המבוקש.

לקוח	ארץ	ותק נשוא הבקשה אצל הלקוח	איש קשר	טלפון

6.2 אנשי קשר ממליצים: יש לצרף פרטי אנשי קשר ממליצים, ככל שניתן, עבור פרויקטים דומים.

שם הממליץ	ארגון	תפקיד	טלפון	דוא"ל	מהות ההתקשרות

7. הערכת עלויות ואומדנים

7.1 לוחות זמנים

זמן משוער נדרש לאספקת הפלטפורמות ותחילת עבודה: _____

7.2 לוחות זמנים

ככל שנדרשות התאמות או פיתוחים, יש לציין אומדן לכמות שעות הפיתוח הנדרשות.

אומדן שעות פיתוח: _____

8. הערכת עלויות: יש לפרט את אומדן העלויות, ככל שניתן, לפי הטבלה שלהלן:

תיאור הפריט	הערכת עלות יחיד	הערכת עלות כוללת	מטבע	הערות
אומדן עלויות				

- האומדן הינו הערכה בלבד. מכבי אינה מחויבת לכמות האומדן או לכמות כלשהיא.
- במידה והמערכת מחולקת למספר מודולים עם עלות נפרדת, יש לציין ולפרט בהתאם.
- במידה וקיימות עלויות לחיבור מערכות / סביבות עבודה / ממשקים נוספים, יש לציין ולפרט בהתאם.
- המחירים אינם כוללים מע"מ

פירוט הספק:

<u>מסמכים שיש לצרף לבקשה:</u>

- הצעה מפורטת וכוללת בהתייחסות לכל הרכיבים הנדרשים בבקשה (כולל הנספחים)
- הצעת מחיר הכוללת את כל העלויות לטובת אספקת המוצרים והשירותים המצוינים בבקשה.
- תקני איכות
- המלצות
- פרוספקטים

נספח א'

דרישות טכנולוגיות

על הספק להתייחס לכל אחת מהדרישות המפורטות להלן. מתחת לכל סעיף יש להשלים פירוט לגבי אופן העמידה בדרישה, מגבלות ככל שקיימות, ותלות ברכיבים או שירותים נוספים, ככל שרלוונטי.

1. **עומסים:** המערכת נדרשת לעמוד בעומסי פעילות גבוהים, ולהציג יכולת גידול תשתיתי פשוטה ומהירה, באופן שיבטיח רציפות תפקודית, ביצועים תקינים וזמני תגובה הולמים גם תחת עומס.

פירוט הספק:

---

2. **אינטגרציה וממשקים:** המערכת נדרשת לתמוך ביכולות אינטגרציה מתקדמות, ובכלל זה:

- יכולת לחשוף שירותים ו- End Points בצורה מהירה בפורמט אחיד, לרבות JSON
- יכולת לצרוך Web Services ממערכות אחרות
- תמיכה ב- REST API
- יתרון ליכולת אינהרנטית להתממשקות ל- Kafka
- יכולת SSO ותמיכה במעבר רציף בין אפליקציה או כלי חיצוני לבין נכסי מכבי, ככל שיידרש

פירוט הספק:

---

3. **יתירות ושרידות:** המערכת נדרשת לממש יכולות יתירות ברכיבים הקריטיים, באופן שיבטיח שרידות, זמינות ורציפות תפקודית גם במקרה של כשל ברכיב בודד.

פירוט הספק:

---

5. **לוגים, ניטור והתרעות:** המערכת נדרשת לתמוך בניהול לוגים מרכזי, הן ברמת התשתית והן ברמת היישום, באופן מובנה ובפורמט JSON לצורך איסוף, העשרה, ניתוח ותצוגה בזמן אמת. בנוסף, נדרשת יכולת ניטור של אירועים חריגים והפקת התרעות בהתאם לספי פעילות שיוגדרו. יתרון יינתן ליכולת התממשקות לפלטפורמות כדוגמת Elastic .

פירוט הספק:

6. **זמינות:** המערכת נדרשת לעמוד בזמינות גבוהה, 24/7, ולספק מענה תשתיתי ואפליקטיבי התומך בדרישה זו. לצורך זה נדרש להציג את הדרישות לעיקרון זה מבחינה תשתיתית / אפליקטיבית

פירוט הספק:

7. **אי-צמידות בין רכיבים(Decoupling) :** המערכת נדרשת לעמוד בעקרון של אי-צמידות בין רכיביה, כך שניתן יהיה להחליף, להזיז או לעדכן רכיבים בצורה פשוטה, מהירה וללא תלות מהותית בין הרכיבים. האינטראקציה בין רכיבי המערכת תתבסס, ככל הניתן, על פרוטוקולים ופורמטים סטנדרטיים ומקובלים, כגון JSON over HTTP ו -RESTful Services, ובשאיפה גם על מנגנונים א-סינכרוניים. עקרון זה נדרש לחול גם על האינטראקציה בין מערכות, באופן שיאפשר המשך תפקוד גם כאשר מערכת מסוימת אינה זמינה.

פירוט הספק:

8. **סטנדרטיזציה ועדכניות טכנולוגית:** רכיבי הארכיטקטורה נדרשים לעמוד בסטנדרטים המקובלים בתעשייה ולהיות מעודכנים לאורך זמן מבחינת גרסאות, תאימות ותחזוקה.

פירוט הספק:

8. **Scalability :** כל רכיב במערכת נדרש לאפשר גידול והרחבה בהתאם לצורך, הן ברמת התשתית והן ברמת הביצועים, לצורך מתן מענה ל- Availability ול -Performance, לרבות Scale Out ו-Scale Up.

פירוט הספק:

9. **בסיסי נתונים:** הפתרון נדרש לתמוך בבסיסי נתונים רלציוניים ו- NoSQL, ככל שהדבר רלוונטי לארכיטקטורת הפתרון.

פירוט הספק:

10. **שירותי ענן:** ככל שהפתרון עושה שימוש בשירותי ענן, לרבות לצורכי גיבוי, יחולו הדרישות הבאות:

- יש לפרט את שם ספק שירותי הענן, מיקום השרתים ומיקום הגיבויים, לרבות מדינה ויבשת
- יש לפרט היכן יישמר מידע המטופלים, לרבות גיבויים
- הסביבה שהוקצתה להפעלת השירות תהיה מופרדת מלקוחות אחרים של ספק שירותי הענן
- יש לפרט את רכיבי אבטחת המידע המיושמים בענן
- המידע הנשמר בענן יישמר כשהוא מוצפן
- ככל שיידרש על ידי מכבי, ההצפנה תתבצע בהתאם למדיניות ההצפנה של מכבי
- יש לפרט אילו תקנים והסמכות קיימים לספק שירותי הענן, ואילו מבדקים מבוצעים על ידו

פירוט הספק:

---

11. אנליטיקה, דוחות ודשבורדים

4.5.1: הפתרון יאפשר יכולות מדידה, ניתוח, הפקת דוחות והצגת דשבורדים עבור מכבי.

4.5.2: הפתרון יאפשר מדידה, ניטור וניתוח של נתונים לאורך מסע המשתמש, לרבות: הרשמה, שימוש, התמדה, נשירה, הישגים, מעידות, שימוש בכלים, אינטראקציות עם תוכן, התקדמות בשלבי התהליך.

4.5.3: הפתרון יאפשר ייצוא נתונים גולמיים והעברת נתונים למערכות BI, אנליטיקה או מחקר של מכבי, ככל שיידרש ובכפוף לאישורים הרלוונטיים.

פירוט הספק:

נספח ב'

אבטחת מידע

1.1 כללי

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

1.1.2 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.

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

1.1.4 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.

1.1.5 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.

1.2 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:

1.2.1 <u>הגדרות</u>

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

1.2.1.2 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

1.2.2 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).

1.2.3 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.

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

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

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

1.2.7 בתחנות העבודה של הספק תשמר אבטחת המידע באופן הבא:

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

1.2.7.2 הכניסה לתחנה תהיה באמצעות USER ID וסיסמא אישית

1.2.7.3 אורך הסיסמא יהיה לפחות שבעה תווים.

1.2.7.4 הסיסמאות יוחלפו כל שלושה חודשים לפחות.

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

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

1.2.7.7 תותקן תכנת הגנה תקנית ומעודכנת כנגד וירוסים.

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

1.2.8 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.

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

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

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

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

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

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

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

1.2.14.2 יבוצע שימוש בפרוטוקול האבטחה WPA 2.

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

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

1.2.15.2 יוגדר לוג אירועים מלא על השימוש בשירות.

1.2.15.3 הגישה לשירות והתעבורה יוצפנו על בסיס הסטנדרטים המקובלים בשוק.

1.3 <u>אבטחת מסמכים</u>

1.3.1 מסמכים ו/או תיקים ו/או כל חומר בעותק קשיח ("Hard copy") אשר הוצאו ממכבי למטרת עבודה יוחזרו חזרה לגורם שעמו מבוצעת ההתקשרות במכבי לצורך גריסה או השמדה מיד בסיום הטיפול בהם.

1.3.2 מסמכים המכילים מידע של מכבי ישמרו נעולים בארונית, מגירה, ארון או כספת שהוקצו לצורך זה בלבד.

1.3.3 הגישה למסמכים אילו תותר רק למי שעבודתם ותפקידם אצל הספק מחייבים זאת, ולכאלו שחתמו על התחייבות לשמירת סודיות מול מכבי.

1.3.4 אין להעביר מסמכים המכילים חומר מודפס של מכבי לגורמים אחרים בכל אמצעי (פקס, דואר ישראל וכו'), ללא אישור כתוב ממכבי.

1.3.5 אין להשאיר מסמכים עם חומר של מכבי על השולחן/במדפסת בסוף יום העבודה.

1.3.6 יש לגרוס מסמכים המכילים מידע של מכבי בתום השימוש בהם.

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

1.4 <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:

1.4.1 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.

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

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

1.4.4 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 .

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

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

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

1.5 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:

1.5.1 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.

1.5.2 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.

1.5.3 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.

1.5.4 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.

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

1.6 ארכיטקטורה

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

1.6.2 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.

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

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

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

1.6.6 הספק יישם את הגדרות האבטחה הבאות:

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

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

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

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

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

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

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

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

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

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

1.6.6.9.2 IPS

1.6.6.9.3 ממשק הפלטפורמה ל- WAF של מכבי

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

1.6.6.9.5 אנטי וירוס - האנטי וירוס יעודכן ברמה יומית.

1.6.6.9.6 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.

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

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

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

1.7 <u>ממשקי Web Service:</u>

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

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

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

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

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

1.7.5 לכל שירות יהיה הזדהות ייחודית והרשאות ייחודיות מול שירותים אחרים.

1.7.6

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

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

1.8 <u>הצפנה</u>

1.8.1 דרישות תעודת הצפנה:

1.8.1.1 תעודת הספק תהיה מ issuer חיצוני ולא CA מקומי

1.8.1.2 אלגוריתם של התעודה תהיה sha256

1.8.1.3 התעודה תכיל CRL Distribution Points

1.8.2 דרישות לגבי ההצפנה:

1.8.2.1 העבודה מול הספק תהיה בתווך TLS ver. 1.2 or above

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

1.9 <u>ניטור אירועים</u>

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

1.9.2 יוגדר ממשק להעברת הלוגים למערכת SIEM של מכבי (QRADAR)

1.9.3 לוג האירועים יוגדר על הבאים:

1.9.3.1 בכל מודול ומערכת שמאחסנת מידע של מכבי.

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

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

1.9.4 לוג אירועים יופעל על האירועים הבאים:

1.9.4.1 כניסות למערכת – מוצלחות או כישלונות.

1.9.4.2 כל גישה לנתונים, כולל קריאה בלבד.

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

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

1.9.4.5 שינוי הגדרות מערכת. כולל שינוי במערכת המשתמשים וההרשאות.

1.9.5 רישום כל אירוע יכלול את הערכים הבאים:

1.9.5.1 מועד ביצוע הפעולה.

1.9.5.2 שם משתמש מבצע הפעולה.

1.9.5.3 כתובת מקור.

1.9.5.4 סוג ה – Client.

1.9.5.5 שם הפעולה.

1.9.5.6 סטטוס – הצלחה\כישלון.

1.9.5.7 תיאור הפעולה.

1.10 <u>פיתוח מאובטח</u>

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

1.10.1 האתר יפותח בסטנדרט פיתוח מאובטח – OWASP-Top 10

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

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

1.12.1 לעבוד עם הכלים הקיימים ברשת מכבי.

1.12.2 לעבוד בתשתיות ה DevOps הקיימות של מכבי.

1.12.3 להורדת כלים נוספים יש לקבל אישור אבטחת מידע.

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

1.12.5 סביבות הפיתוח לא יהיו נגישות בשום אופן לרשת האינטרנט.

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

1.13.1

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

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

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

1.13.5 חל איסור לבצע שימוש במידע חסוי/חסוי ביותר/ מידע אישי מזוהה כTest Data בתהליכי QA ופיתוח. לתהליכים אלו יש להשתמש בData אנונימי או בData רנדומלי בלבד

1.13.6 חריגה מאופשרת באישור מראש על ידי מכבי שירותי בריאות.

1.14 יש לבצע מבדקי חדירות לפני עלייה לאוויר:

1.14.1 יוגדרו לבדיקה משתמשים וסביבה לביצוע הבדיקה.

1.14.2 לאחר הבדיקה יפורסם דוח ממצאים.

1.14.3 לאחר ישיבת תיקוף יש לטפל בממצאים ברמה גבוהה ובינונית.

1.14.4 לאחר הטיפול בממצאים יש לבצע בדיקת חדירות חוזרת.

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

1.15 <u>אבטחת מידע בענן:</u>

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

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

1.15.2 ספק הענן יהיה ב- EU Region בלבד

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

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

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

1.15.6 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.

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

1.15.8 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.

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

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

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

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

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

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

1.15.11.4 גישת משתמשים תעבור דרך מערכת Proxy של מכבי.

1.15.11.5 ההזדהות תתאפשר מכתובות IP של מכבי בלבד.

1.15.12 <u>אחסון מידע</u>

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

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

1.15.13 <u>הצפנת המידע</u>

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

1.15.13.2 ההצפנה תבוצע בהתאם לסטנדרטים המקובלים בשוק.

1.15.13.3 מפתחות ההצפנה יישמרו באופן בלעדי בידי הארגון במידת האפשר.

1.15.14 ניטור אירועים

1.15.14.1 ניטור אירועים על פי המוגדר בסעיף ניטור אירועים

1.15.15 העברת מידע

1.15.15.1 העברת המידע תבוצע בתווך מזוהה ומוצפן.

1.15.16 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.

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

1.15.18 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.

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

1.15.20 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.

1.15.21 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.

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