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

04/08/2026

בקשה לקבלת מידע (RFI)

מערכת POINT-OF-CARE לזיהוי VAGINITIS

(להלן – "הבקשה")

1. כללי

1.1. מכבי שירותי בריאות (להלן –" **מכבי** ") מעוניינת לקבל מידע על ספקים המציעים מערכת בטכנולוגיית POINT-OF-CARE (**POC**), שמבוססת על סורק שולחני, לזיהוי אבחנות שונות של VAGINITIS, לתפעול עצמאי ע"י מטפלי מכבי (להלן – **"השירותים"),** כמפורט בבקשה.

1.2. את המידע יש למלא על גבי מסמך של המציע ולשלוח אל **שחר מסר** לדואר אלקטרוני **messer_s@mac.org.il** עד 25.08.2026.

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.

2. רקע

2.1. מכבי שירותי בריאות מעוניינת לעשות שימוש במערכת POC לאבחון מהיר של דלקות נרתיק זיהומיות - VAGINITIS.

2.2. מכבי מעוניינת לבחון את סביבת השוק של מערכות לזיהוי דלקות נרתיקיות' הכרת היכולות המוצעות במערכות השונות לביצוע הבדיקות ומידת התאמתן לצרכי הקופה המשתנים.

2.3. מתכונת העבודה במכבי הינה פנייה של נשים סימפטומטיות למוקדי רפואת נשים או לרופא נשים בקהילה, ביצוע הבדיקה בעזרת מטוש בו במקום במתכונת POC וקבלת תשובה לגבי מקור הזיהום על מנת שיותאם טיפול מיטבי כמפורט בסעיף 3.7 להלן.

2.4. בשלב ראשון של הפרויקט הבדיקה תתבצע רק במסגרת המוקדים במכבי. אבל ההפניה יכולה להיות גם מרופא הקהילה.

2.5. יש להעביר מידע לגבי 'מעטפת השירות' המלאה המלווה את המוצר, כגון הדרכה לשימוש במערכת, תמיכה שוטפת בתפעול העצמאי ע"י מכבי, אופן הטיפול בתקלות, שדרוג גרסאות וכד'.

3. פרופיל ודרישות כלליות ממציע ההצעה (להלן "החברה") ומהמערכת

יש להעביר פירוט במסמך מצורף, לגבי עמידת החברה בכל המפורט להלן

3.1. חברה שמספקת מערכת טכנולוגית POINT-OF-CARE לזיהוי אבחנות שונות של VAGINITIS הכוללת לכל הפחות את האבחנות הבאות :

- וגיניטיס חיידקי (BV)
- קנדידה אלביקנס
- קנדידה שאיננה אלביקנס
- טריכומונס
- אטרופיה נרתיקית
- DIV
- וגיניטיס ציטולוטי

3.2. לחברה ניסיון מוכח באספקת המוצר ומעטפת השירות לחברות וארגונים העושים שימוש במערכת בארץ ובעולם.

3.3. למערכת יכולת תמיכה בהיקפים של עשרות אלפי בדיקות בשנה.

3.4. יכולת תמיכה מרחוק במשתמשים פנים ארגוניים.

3.5. המערכת עם יכולת לשדר את תוצאות הבדיקה ישירות למערכות מכבי באופן מאובטח – כמפורט בנספח א' להלן.

3.6. החברה תידרש להציג מחויבות לאבטחת מידע ופרטיות המשתמשים כמפורט בנספח ב' להלן.

3.7. המערכת תתאים לתהליך הבא:

- המטופלת מגיעה עם תלונה סימפטומטית המעידה על דלקת נרתיק
- תילקח דגימה של הפרשה נרתיקית עם הדוגם הייעודי של המערכת או ע"י מטוש בבדיקה עצמית של המטופלת או בבדיקת רופא במסגרת בדיקה נרתיקית.
- המטוש מועבר לסורק ע"י עובדת המעבדה או אחות.
- הנתונים נשלחים באפליקציה הייעודית לענן באלגוריתם באופן אוטומטי אבחנה עם תמונת המצב המאובחן נשלחת מיידית לרופא או לגורם הבודק.
- רופא מתאים באופן מידי את הטיפול המתאים למצב המאובחן.

4. מפרט מבוקש

4.1. דרישות ממערכת זיהוי דלקת נרתיקית

4.1.1. יכולת ביצוע בדיקות לזיהוי דלקת נרתיקית ב point of care setting

4.1.2. רספונסיבי - יכולת למענה מותאם ממחשב נייח או נייד טאבלט.

4.1.3. הנחיות לבדיקה בשפות שונות – נבקש הצגה של היכולות.

4.1.4. יכולת להצגת נתוני המשובים הפרטניים און ליין – נבקש הצגת אופן שיקוף הנתונים עבור מבצע הבדיקה און ליין של תוצאות הבדיקות

4.1.5. דשבורד ניהולי/מקצועי - הצגת יכולות מידע וניהול של הבדיקות במערכת – כגון מעקב און ליין על כמות הבדיקות, פילוח תוצאות הבדיקות החיוביות

4.2. דרישות נוספות:

4.2.1. הדרכה והטמעה מובנית ומסודרת לצוותים , כולל תמיכה טכנית אונליין.

4.3. דרישות טכניות עיקריות:

4.3.1. ממשק משתמש ידידותי ואינטואיטיבי.

4.3.2. גיבוי למידע הנאסף – פעם ביום או יותר.

4.3.3. במערכת – התכנות להעברת כל המידע הנאסף (נתוני הגלם) למכבי באופן שוטף, און ליין, בסיום ביצוע הבדיקה. העברת המידע במבנה נתונים שהוגדר ע"י מכבי.

4.3.4. המערכת מאפשרת התממשקות ושליחת התוצאות במסרון, מספק המסרונים של מכבי. – אופציה בלבד –

4.3.5. מערכת אבטחת מידע מתקדמת להגנה על מידע אישי רגיש, לרבות עמידה בסטנדרטים הנדרשים על פי נספח ב' מצ"ב.

4.4. התייחסות להיבטים טכנולוגיים: במסגרת המענה לבקשה יש להתייחס לשני הנספחים המצורפים :

- נספח א - דרישות טכנולוגיות
- נספח ב - אבטחת מידע

5. פרטי המציע :

5.1. הספק המשיב:_____

5.2. ותק וניסיון בארץ /בעולם:_____

5.3. פירוט היכולות המוצעות במערכות (סוגי זיהומים).

5.4. כל נתון וחומר רלוונטי נוסף.

5.5. לקוחות מרכזיים (שמשתמשים במערכת) :

לקוח	ארץ	ותק נשוא הבקשה אצל הלקוח	סוגי סקרים והיקפם	איש קשר	טלפון

5.6. הערכת עלויות ואומדנים

5.6.1. יש להציג את מודל התמחור בצורה מפורטת ככל הניתן, לרבות רכיבי עלויות.

5.6.2. במידה והמערכת מחולקת למספר מודולים עם עלות נפרדת, יש לציין ולפרט בהתאם.

5.6.3. במידה וקיימות עלויות לחיבור מערכות / סביבות עבודה / ממשקים נוספים, יש לציין ולפרט בהתאם.

6. מסמכים שיש לצרף לבקשה:

6.1. הצעה מפורטת וכוללת, בהתייחסות **לכל** הרכיבים הנדרשים בבקשה (כולל התייחסות לנספחים).

6.2. הצעת מחיר הכוללת את כל העלויות לטובת אספקת השירותים המצוינים בבקשה, כולל אבני דרך ותמחור שעות במידה ונדרש.

6.3. המלצות.

6.4. מצגות תכלית – ככל שיש.

6.5. מידע כללי על החברה – כמות עובדים, פרופיל העובדים, מנהלי הלקוחות.

נספח א'

דרישות טכנולוגיות

1. **ארכיטקטורת מערכת:**

האם מערכת בענן
תמיכה בעבודה בארגונים גדולים (Multi-tenant?).
זמינות גבוהה (99.9% ומעלה), התאוששות מאסון.

דרישה	תיאור	מענה הספק- יש לתת מענה מפורט
פתרון ענן מאובטח	ארכיטקטורת פתרון מבוסס ענן העונה על דרישות אבטחה ותקנים רלוונטיים. יש לציין באיזה עננים(AWS, GCP, AZURE וכו') ואיזה regions ניתן לצרוך את השירות עבור לקוחות ישראליים	
אפשרויות פריסה	מהן אפשרויות פריסת המוצר ענן, לוקאלי, היברדי פרטו מה האפשרויות השונות והמלצות עבור מכבי אם יש.	
עמידה ברגולציה ותקנים רלוונטיים	עמידה בתקנים רגולטוריים ותקני אבטחה עבור סוג הפתרון (ענן/לוקאלי)	
ארכיטקטורה גמישה	יכולת הרחבה והתאמה לצרכים משתנים האם Cloud native עבודה בקונטיינרK8S, Docker	
זמינות	פירוט % זמינות עליו מתחייב הספק	
עבודה מול בסיסי מידע לוקאלים	יכולת המערכת לשליפת/קבלת מידע ממאגרי המידע של מכבי (כגון Data warehouse) ללא יצירת שכבת מידע נוספת ומותאמת עבור המוצר	

2. **מפרטי ביצועים**

כמות משתמשים במקביל.
מספר בדיקות בו זמנית.
זמני תגובה צפויים.

דרישה	תיאור	מענה הספק- יש לתת מענה מפורט
זמני תגובה	פירוט זמני תגובה ממוצעים (כגון הרצת חוק עם X פרמטרים וקבלת תשובה עד 2 שניות) שתפו במידת האפשר בתוצאות ה-benchmark שבצעתם לבדיקות עומסים. רלוונטי לכלל הסעיפים בחלק זה.	
יכולת הרצת חוקים בו זמנית	כמות חוקים היכולים לרוץ בו זמנית (concurrent)	
עיבוד אצווה	זמני תגובה ממוצעים עבור הרצת חוקים על אצווה (Batch)	
כלים לניטור ביצועים	כלים לניטור ביצועי המערכת. האם עושים שימוש בסטנדרטים דוגמת OpenTelemetry? פרטו	

3. מפרטי ביצועים

דרישה	תיאור	מענה הספק- יש לתת מענה מפורט
פרוטוקולי תקשורת סטנדרטים	תמיכה בפרוטוקולי תקשורת סטנדרטיים (כגון REST, SOAP API)	
יכולת עיבוד אצווה (Batch)	יכולת הפעלת חוקים על אצווה גדולה בצורה יעילה	
אינטגרציה מבוססת API	חיבור פשוט למערכות חיצוניות באמצעות ממשקי API תמיכה ב-OpenAPI האם כל הפונקציונאליות של המערכת מתאפשרת גם באמצעות API? אם לא מה היכולות שלא נתמכות ב-API?	
תמיכה במקורות מידע מרובים	יכולת התחברות למגוון מקורות מידע	
מעקב ניטור שגיאות והתראות	מערכת ניטור ודיווח שגיאות בתהליכי אינטגרציה	
עיבוד נתונים בזמן אמת	יכולת עיבוד והתממשקות בזמן אמת	

נספח ב'

דרישות אבטחת מידע

1. <u>פרסום, שמירת סודיות ואבטחת מידע</u>

1.1. כל פרסום בקשר להסכם זה ו/או שימוש בשמה של מכבי, לרבות בסימני המסחר שלה, כפופים לקבלת אישורה מראש ובכתב של מכבי.

1.2. **<u>דרישות לסודיות</u>**:

הזוכה מצהיר ומתחייב כדלקמן:

1.2.1. לשמור על סודיות מוחלטת ביחס לכל המידע שנכלל במסמכי ההסכם וכן ביחס לכל ידיעה בקשר עם ביצוע הסכם זה ולכל מידע על ושל מכבי, עובדיה, מבוטחיה, שיטות עבודתה, נתוניה הכספיים, מידע על ספקיה, מידע רפואי, מידע ניהולי, מידע עסקי, מידע פיננסי וכיו"ב נתונים, אשר יגיעו לידיעתו בתוקף או במהלך או אגב או במסגרת ביצוע התחייבויות הזוכה על-פי האמור במסמכי הסכם זה, תוך תקופת ההתקשרות, לפני תחילתה או לאחר סיומה (להלן "**המידע**").

1.2.2. למנוע כל פרסום ו/או גילוי של המידע בכל דרך שהיא ובכל זמן שהוא, ולא למסור ו/או להעביר את מהידע לכל צד שלישי כלשהו, אלא אם קיבל אישור ספציפי, לכל נושא בנפרד, בכתב, מאת מכבי ובהתאם לאישור שניתן.

1.2.3. לעשות את כל הסידורים הדרושים לשמירת המידע, להגביל את הגישה למידע אך ורק לעובדי הזוכה המורשים לכך, ולדאוג לכך שכל עובדי הזוכה, נותני שירותים והמועסקים על ידו ומטעמו לצורך ביצוע התחייבויותיו על-פי ההסכם יחתמו על כתב התחייבות אישי לשמירת סודיות כלפי הזוכה (בכל עת), בנוסח המחייב אותם לעמוד בהתחייבויות הזוכה לשמירת סודיות המפורטות בהסכם זה, וכן כלפי מכבי (בהתאם לדרישה מפורשת ולנוסח שיומצא על-ידי מכבי).

מובהר בזאת, למען הסר ספק, כי הזוכה יהא אחראי כלפי מכבי למילוי האמור על-ידי עובדיו ו/או הפועלים מטעמו או עבורו.

1.2.4. חובת שמירת הסודיות המפורטת לעיל לא תחול על:

1.2.4.1. מידע שהיה בידי הזוכה ו/או בידי עובדיו ו/או נותני השירות מטעמו טרם ההתקשרות בהסכם זה שלא עקב הפרת התחייבות לשמירת סודיות;

1.2.4.2. מידע שנתקבל מצד ג' באופן עצמאי שלא עקב הפרת התחייבות לשמירת סודיות;

1.2.4.3. מידע שהוא או הפך נחלת הכלל שלא בגין הפרת התחייבות לסודיות של הזוכה.

1.2.4.4. מידע שחובה לגלותו על-פי דין או על-פי צו מרשות שיפוטית מוסמכת, ובלבד שהזוכה הודיע למכבי ללא דיחוי אודות צו כאמור, ואפשר לה להתגונן מפניו.

1.2.5. כי ידוע לו והוא מסכים שכל המידע הוא בבעלותה הבלעדית של מכבי, וכי הזוכה לא יהא רשאי לעשות בו כל שימוש שאינו לצורך ביצוע ההסכם.

1.2.6. כי ידוע לו שייתכן והוא ייחשף גם למידע רגיש ביותר, לרבות מידע אשר קיימת לגביו התחייבות מפורשת או משתמעת של מכבי כלפי צדדים שלישיים לשמור עליו בסודיות, ואשר גילויו לאחרים או שימוש בו שלא לצורך ביצוע ההסכם עלול לגרום למכבי נזקים והפסדים ולהפרת התחייבות לשמירת המידע בסודיות, וכי הזוכה מודע לכך שהמידע הינו חלק מנכסיה של מכבי.

1.2.7. כי ידועות לו הוראות הדין הקובעות את חובת שמירת הסודיות, והוא מודע לסנקציות האזרחיות והפליליות (בנוסף לצעדים בגין הפרת ההסכם) להן הוא צפוי אם הוא או מי מעובדיו מי מטעמו יפר הוראות אלו, לרבות (אך לא רק) הוראות חוק הגנת הפרטיות,

התשמ"א-1981 ותקנותיו, חוק זכויות החולה, התשנ"ו-1996, חוק העונשין, התשל"ז-1977, וכל דין רלבנטי נוסף.

1.3. **<u>דרישות אבטחת מידע</u>**:

הזוכה מצהיר ומתחייב כדלקמן:

כללי

1.3.1. אצל הספק יוגדר איש קשר אחראי לאבטחת המידע שבאחריותו לוודא את יישומן של הדרישות שיובאו להלן.

1.3.2. הספק מתחייב כי הנו בעל הסמכה לתקן בינלאומי לאבטחת מידע – ISO27001 או לתקן לאבטחת מידע במוסדות בריאות ISO27799.

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

1.3.4. 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.

1.3.5. 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.

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

1.3.7. 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.

1.3.8. יש לדווח למנהל אבטחת המידע והגנת הסייבר במכבי בכל חשד לאירוע אבטחת מידע בעל השפעה על המידע של מכבי.

1.3.9. 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.

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

1.3.11. כל אתרי מכבי יעברו בדיקות PT ע"י מכבי. הספק מתחייב לתקן כל ממצא מהותי שיעלה בבדיקות על פי הגדרת מכבי.

1.3.12. הספק מתחייב לדווח על כל אירוע אבטחה הרלוונטי למידע של מכבי

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:

1.3.13. 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, ניתן לקשר את מחשבי הספק אשר אינם משמשים לאחסון המידע של מכבי לרשת האינטרנט.

1.3.14. 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.

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

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

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

1.3.18. בתחנות העבודה של הספק תשמר אבטחת המידע באופן הבא:

1.3.18.1. לא יישמרו קבצי מכבי על הדיסק הקשיח של התחנה (למעט לגבי חברה או יחיד ללא רשת משתמשים).
1.3.18.2. הכניסה לתחנה תהיה באמצעות USER ID וסיסמא אישית .
1.3.18.3. אורך הסיסמא יהיה לפחות שבעה תווים.
1.3.18.4. הסיסמאות יוחלפו כל שלושה חודשים לפחות.
1.3.18.5. התחנה תינעל אוטומטית לאחר 5 שגיאות רצופות בהקשת הסיסמא.
1.3.18.6. בכל תחנה יותקן נועל מסך עם סיסמא שיופעל לאחר 20 דקות לכל היותר.
1.3.18.7. תותקן תכנת הגנה תקנית ומעודכנת כנגד וירוסים.
1.3.18.8. מערכת ההפעלה המותקנת על התחנה מעודכנת בעדכוני האבטחה האחרונים שהופצו על ידי היצרן.

1.3.19. לא יוצאו דיסקים משרתי הספק או ממחשבים אישיים (למעט לגבי חברה או יחיד ללא רשת משתמשים) לתיקון או לכל מטרה אחרת כשעליהם נמצאים קבצים המכילים מידע של מכבי .במקרה כזה יש למחוק את המידע ולפרמט את הדיסק.

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

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

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

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

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

1.3.25. הספק מתחייב לאפשר לנציג מכבי לערוך ביקורת אבטחה בכל עת. הביקורת תבוצע בתאום עם הספק.

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

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

1.3.26.2. יבוצע שימוש בפרוטוקול WPA 2.

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

1.3.27.1. יבוצע "זיהוי חזק" כפול בעת הגישה לשירות.

1.3.27.2. יוגדר לוג אירועים על השימוש בשירות.

1.3.28. הגישה לשירות תבוצע על ידי שימוש בהצפנה על בסיס הסטנדרטים המקובלים בשוק.

1.3.29. ארכיקטורה

1.3.29.1. האתרים המשמשים את פתרון הסקרים אשר נשלחים למבוטחי מכבי יהיו תחת Domain מכבי (כלומר הURL של האתרים יהיו בDomain מכבי).

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

1.3.29.3. שליחת המיילים יועברו מכתובת של מכבי בלבד - maccabi4u.co.il@. לצורך כך הספק מתחייב להעביר כתובות IP למכבי לצורך הגדרת SPF.

1.3.29.4. הלינק למילוי שאלון ע"י משתמשי הקצה יהיה מבוסס SSL

1.3.29.5. סקרים המצריכים זיהוי מבוטח יבוצעו על ידי אינטגרציה מלאה למערך הזדהות המבוטחים במכבי בפרוטוקול SAML

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

1.3.29.7. הספק יישם את הגדרות האבטחה הבאות:

1.3.29.7.1. האתרים המשמשים את פתרון הסקרים אשר נשלחים למבוטחי מכבי ימוגנו על ידי Web application firewall , ופתרון DDOS.

1.3.29.7.2. ממשק ניהול (מכל סוג) לא יהיה נגיש לכל כתובות האינטרנט, אלא יפתח ב FW רק לכתובות ספציפיות.

1.3.29.7.3. כל נתוני הלקוח ישמרו מחוץ לשרת ה WEB בשרת מסד הנתונים ייעודי .

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

1.3.29.7.5. מערכת ה Active Directory או מערכת ניהול הרשת המקבילה תשב בסגמנט ייעודי מופרד ב FW מסגמנט שרת ה WEB. סיגמנט זה יהיה חסום לגישה אל ומ – האינטרנט.

1.3.29.7.6. שירותי מכבי יפעלו בשרתים ייעודים למכבי, בהם אינם שותפים גורמים נוספים. למען הסר ספק דרישה זו לכלל מרכיבי השירות.

1.3.30. ממשקי Web Service

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

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

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

1.3.30.3. מכבי תוכל לספק תעודות דיגיטליות לכל הצדדים בתהליך.

1.3.30.4. התשתיתיים והאפליקטיביים, הכוללים את תשתיות הרשת (Active Directory לדוגמא), מסדי הנתונים, האפליקציה, וה- WEB.

1.3.31. הצפנה

1.3.31.1. דרישות תעודת הצפנה:

1.3.31.1.1. תעודת הספק תהיה מ issuer חיצוני ולא CA מקומי

1.3.31.1.2. אלגוריתם של התעודה תהיה sha256

1.3.31.1.3. התעודה תכיל CRL Distribution Points

1.3.31.2. דרישות לגבי ההצפנה:

1.3.31.2.1. העבודה מול הספק תהיה בתווך SSL

1.3.31.2.2. יכולת התממשקות מול AZURE

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

1.3.32 סביבות הפיתוח:

1.3.32.1 האתר יפותח בסטנדרט פיתוח מאובטח – OWASP-Top 10

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

1.3.32.3. סביבות הפיתוח לא יהיו נגישות בשום אופן לרשת האינטרנט.

1.3.32.4. חריגה מאופשרת באישור מראש על ידי מכבי שירותי בריאות

גישה לרשת ולמערכות מכבי

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:

1.3.33. 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.

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

1.3.35. הפעולות המבוצעות בעמדת עבודה המחוברת למערכת מכבי מנוטרות באמצעות מערכות הניטור והבקרה במכבי.

1.3.36. על עובד הספק הנעדר מעמדת העבודה להקפיד לנעול אותה באמצעות שומר מסך מוגן סיסמא.

1.3.37. 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 .

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

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

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

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:

1.3.41. כל כללי אבטחת המידע החלים על עמדת העבודה יחולו גם על אמצעי המחשוב הנייד.

1.3.42. 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.

1.3.43. 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.

1.3.44. 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.

1.3.45. 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.

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

1.3.47. הספק מתחייב לאפשר לנציג מכבי לערוך ביקורת על אבטחת אמצעי המחשוב הנייד בכל עת. הביקורת תבוצע בתאום מראש מול הספק.

אבטחת מידע בענן:

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

1.3.48. ספק הענן יהיה ב- EU Region בלבד

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

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

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

1.3.52. 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.

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

1.3.54. 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.

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

1.3.56. 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, PCI , חוק הגנת הפרטיות.

ניהול זהויות והרשאות בענן:

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

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

אחסון מידע

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

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

הצפנת המידע

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

1.3.62. ההצפנה תבוצע בהתאם לסטנדרטים המקובלים בשוק.

1.3.63. מפתחות ההצפנה יישמרו באופן בלעדי בידי הארגון במידת האפשר.

ניטור אירועים

1.3.64. יוגדר ויופעל לוג אירועים מלא על כלל האירועים בכלל מרכיבי שירות הענן.

1.3.65. לוג האירועים יוגדר על הבאים:

1.3.65.1. בכל מודול ומערכת שמאחסנת מידע של מכבי.

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

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

1.3.66. לוג אירועים יופעל על האירועים הבאים:

1.3.66.1. כניסות למערכת – מוצלחות או כישלונות.

1.3.66.2. כל גישה לנתונים, כולל קריאה בלבד.

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

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

1.3.66.5. שינוי הגדרות מערכת. כולל שינוי במערכת המשתמשים וההרשאות.

1.3.67. רישום כל אירוע יכלול את הערכים הבאים:

1.3.67.1. מועד ביצוע הפעולה.

1.3.67.2. שם משתמש מבצע הפעולה.

1.3.67.3. כתובת מקור.

1.3.67.4. סוג ה – Client.

1.3.67.5. שם הפעולה.

1.3.67.6. סטטוס – הצלחה\כישלון.

1.3.67.7. תיאור הפעולה.

העברת מידע מהארגון לשירותי הענן

1.3.68. העברת המידע תבוצע בתווך מזוהה ומוצפן.