

תאריך: 11.07.2022

## בקשה לקבלת מידע (RFI)

### **עבור טכנולוגיית סרטונים מותאמים אישית (להלן – "הבקשה")**

#### **1. כללי**

1.1. מכבי שירותי בריאות (להלן – "מכבי") מעוניינת לקבל מידע בנושא: "טכנולוגיית סרטונים מותאמים אישית" (להלן – "המוצרים והשירותים"), כמפורט בבקשה.

1.2. את המידע יש למלא על גבי המסמך מצ"ב / מסמך של המציע ולשלוח אל שחר מסר לדואר אלקטרוני [messer\\_s@mac.org.il](mailto:messer_s@mac.org.il) עד לתאריך 25.07.2022

1.3. פרסום הבקשה למידע אינו מבטל את זכותה של מכבי להמשיך 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.

1.4. 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.

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

1.6. מכבי שומרת לעצמה את הזכות לקיים פגישות הבהרה עם המשיב ו/או לדחות את המענה, הכל בהתאם לשיקול דעתה הבלעדי.

1.7. לאחר בחינת המידע והתרשמות, מכבי תעשה במידע זה כראות עיניה, לרבות שימוש לצורך כתיבת מפרטים, מכרז או מסמך דרישות כלשהן ו/או כל שימוש אחר.

תאריך: 11.07.2022

- 1.8. מכבי שומרת לעצמה את הזכות לקיים מפגש אליו יוזמנו המשיבים שנטלו חלק בשלב זה של הפנייה לקבלת מידע או מי מהם, לפי שיקול דעתה הבלעדי של מכבי.
- 1.9. מכבי שומרת לעצמה את הזכות לפרסם פנייה נוספת ו/או לפרסם מכרז ו/או לא להתקשר בהסכם כלשהו עם מי מהמשיבים.
- 1.10. 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 וענייניים.
- 1.11. מכבי תהא רשאית לעשות שימוש בכל מידע (כולו או חלקו) שיימסר במסגרת תשובה לבקשה לקבלת מידע זו ולמוסר המידע לא תהיינה טענות בדבר זכויות יוצרים מכל מין וסוג שהם.
- 1.12. במידה הצורך ולשיקול דעתה המקצועי של מכבי, המשיב מתחייב לספק, ללא חיוב, מערכת לצורך ביצוע פיילוט.
- 1.13. 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.

תאריך: 11.07.2022

## 2. תיאור כללי של נושא הבקשה והמפרט המבוקש

### 2.1. רקע

כחלק מהתכנית לשיפור העצמת המטופל ומעורבות מטופל, מכבי מעוניינת לבחון שימוש בשירות SAAS המייצר סרטונים מותאמים אישית עבור מסעות מטופל קליניים. המערכת עתידה לספק מידע רפואי למטופלים בפורמט של סרטון עבור פרוצדורות קליניות ופרה קליניות, וכן עבור פרוצדורות אדמיניסטרטיביות. הסרטונים צריכים להיות מופקים On The Fly לפי סט הגדרות שייקבע מראש ויתקבל באופן אוטומטי ממערכות מכבי.

### 2.2. הנחיות למילוי הבקשה

2.2.1. על המשיב לפנייה לקבלת מידע לעמוד בכל הדרישות והתנאים המפורטים מטה.

2.2.2. על המענה לתאר את תכונות המערכת ולהתייחס לכל אחד מהסעיפים להלן.

2.2.3. בהתייחסות יש לציין האם המאפיין קיים במוצר הבסיסי / דורש פיתוח / לא אפשרי / קיים

ב- Roadmap הפיתוחי של המוצר.

2.2.4. במידה ונדרש פיתוח יש להרחיב את משמעות הנושא.

### 2.3. המפרט המבוקש

2.3.1. מערכת SAAS להפקה אוטומטית של סרטונים מותאמים אישית להנחיות למטופלים לפני

בדיקה או הנחיות לאחר\לפני ביקור רופא עבור מצבים קליניים שונים.

2.3.2. תמיכה בלפחות 5 פרוצדורות קליניות משמעותיות \ הכנה לבדיקות שונות.

2.3.3. יכולת ליצור סרטונים אינטראקטיביים, המשתנים לפי האינטראקציה של המטופל.

2.3.4. יכולת אוטומציה מלאה בהפקת סרטונים: תהליך קיים (API) של קבלת דאטה רלוונטי

מגיליון רפואי של מטופל או ממערכת מידע אחרת, והפקה אוטומטית של סרטון פרסונלי

בהתבסס על הדאטה המתקבל.

תאריך: 11.07.2022

- 2.3.5. יכולת להפקת סרטונים חצי אוטומטים ע"י עובד מכבי. כלומר אפשרות לערוך ידנית סרטונים שלא באמצעות עץ החלטה.
- 2.3.6. כל התוכן בפלטפורמה תומך בעברית, כלומר מדובר לעברית במידה ומדובר באנימציה, או מוקרא ע"י שחקנים בעברית אם מדובר ב Live Action.
- 2.3.7. לפלטפורמה יהיה ממשק התחברות (API) למערכות מכבי נוספות ככל שיידרש (CRM, גליון רפואי, אחר)
- 2.3.8. הפלטפורמה תציג יכולת התממה, כך שלא יעבור מידע מזהה של מטופלים למערכות החברה.
- 2.3.9. הפלטפורמה תשב על ענן ישראלי, אירופאי או אמריקאי.
- 2.3.10. תוצרי הפלטפורמה, הסרטונים למטופל יוצגו למטופלים על כלל מכשירי הקצה, ביניהם: מחשבים אישיים (דפדפני כרום, ספארי, פיירפוקס, אדג'), מכשירים ניידים וטאבלטים (דפדפני ספארי, כרום) וכן בתוך אפליקציית מכבי.
- 2.3.11. עמידה בכל דרישות אבטחת מידע כמפורט בנספח א' לבקשה.

תאריך: 11.07.2022

### 3. טופס הבקשה :

- 3.1. התאגיד המשיב: \_\_\_\_\_
- 3.2. שם החברה: \_\_\_\_\_
- 3.3. שם המערכת המוצעת: \_\_\_\_\_
- 3.4. תומך בעברית: \_\_\_\_\_
- 3.5. ותק הטכנולוגיה בארץ / בעולם: \_\_\_\_\_
- 3.6. תקנים קיימים למערכת המוצעת, כולל אבטחת מידע: \_\_\_\_\_
- 3.7. כל נתון וחומר טכני רלוונטי נוסף. \_\_\_\_\_

### 4. 5 לקוחות מרכזיים במגזר הבריאות (שבוצעה עבורם הטמעה מלאה של המערכת) :

| לקוח | ארץ | ותק נשוא הבקשה אצל<br>הלקוח | איש קשר | טלפון |
|------|-----|-----------------------------|---------|-------|
|      |     |                             |         |       |
|      |     |                             |         |       |
|      |     |                             |         |       |
|      |     |                             |         |       |
|      |     |                             |         |       |

תאריך: 11.07.2022

## 5. הערכת עלויות ואומדנים

5.1. זמן משוער נדרש לאספקת המערכת ותחילת עבודה: \_\_\_\_\_

5.2. הגדרת אומדן לכמות שעות פיתוח נדרשות: \_\_\_\_\_

5.3. הערכת עלויות:

| הערות     | מטבע | הערכת עלות כוללת | הערכת עלות יחיד | תיאור הפריט                                                                                   |
|-----------|------|------------------|-----------------|-----------------------------------------------------------------------------------------------|
| תוכן      |      |                  |                 |                                                                                               |
|           |      |                  |                 | <ul style="list-style-type: none"> <li>הפקת תוכן עבור מסע מטופל שאינו קיים במערכת.</li> </ul> |
| מודל עסקי |      |                  |                 |                                                                                               |
|           |      | (מדרגות)         |                 | מודל עסקי ותמחור לפי SAAS עלו                                                                 |
|           |      | (מדרגות)         |                 | מודל עסקי ותמחור לפי Fixed fee מודל                                                           |
|           |      |                  |                 | רישוי אחר (אם נדרש)                                                                           |
| נוספות    |      |                  |                 |                                                                                               |
|           |      |                  |                 | אינטגרציה למערכות מכבי                                                                        |
|           |      |                  |                 | הדרכה והכשרה                                                                                  |
|           |      |                  |                 | שונות - יש לפרט בעמודת הערות                                                                  |
|           |      |                  |                 | שם ספק ענן + מיקום                                                                            |
|           |      |                  |                 | SLA                                                                                           |
|           |      |                  |                 | תמיכה בתשתיות הנדרשות                                                                         |
|           |      |                  |                 | התממת מידע                                                                                    |
|           |      |                  |                 | אבטחת מידע:                                                                                   |

תאריך: 11.07.2022

5.3.1. האומדן הינו הערכה בלבד. מכבי אינה מחויבת לכמות האומדן או לכמות

כלשהיא.

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

בהתאם.

5.3.3. במידה וקיימות עלויות לחיבור מערכות / סביבות עבודה / ממשקים נוספים, יש

לציין ולפרט בהתאם.

5.3.4. המחירים אינם כוללים מע"מ

5.4. מסמכים שיש לצרף לבקשה:

- תקני איכות
- המלצות
- פרוספקטים
- כל מידע רלוונטי אחר (כגון: ניסיון שלו בתכנון, הטמעה ותפעול המערכת)

תאריך: 11.07.2022

## נספח א' – דרישות אבטחת מידע

להלן דרישות אבטחת מידע מהמערכת:

### 1.1. כללי

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

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

1.1.3. הספק מתחייב להעביר למכבי עד רבעון מיום חתימת ההסכם, תעודת "ספק מאושר" לאבטחת מידע מטעם גוף התעדה מורשה מטעם מערך הסייבר הלאומי. התעודה מנופקת לאחר מבדק שמבוצע על ידי בודק תאימות סייבר מוסמך לשרשרת אספקה ארגונית של מערך הסייבר הלאומי. המבדק יערך על פי שאלון ספקים של מערך הסייבר הלאומי, לקטגוריות הבאות: דרישות רוחביות (טיפול במידע+ עבודה בחצרות הלקוח), גישה מרחוק, פיתוח תוכנה, אחסון מידע בענן, אחסון אתרים (Hosting). להלן קישור לרשימת בודקים מוסמכים של מערך הגנת הסייבר לתיאום הסקר: [https://www.gov.il/he/Departments/General/bodkim\\_2019](https://www.gov.il/he/Departments/General/bodkim_2019) למען הסר ספק הפניה לבדק, המבדק ומימון הפעילות יבוצעו באחריות הספק, ללא מעורבות מכבי. דרישה זו הנה דרישה רגולטורית בסיסית לכל ספק של מכבי כארגון בריאות, על פי דרישות מב"ר.

### 2. נהלי אבטחת מידע

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

2.1.2. במקרים שבהם הספק מקבל ממכבי מידע המכיל פרטים אודות חברי מכבי ו/או 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.

2.1.3. 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.

תאריך: 11.07.2022

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

2.1.5. 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.

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

2.1.7. 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.

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

2.1.9. 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.

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

## 2.2. אבטחת מידע לוגית

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

### 2.2.2. הגדרות

2.2.2.1. מידע חסוי - מידע עסקי/ מידע רפואי/ מידע על עובדי מכבי

2.2.2.2. 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

2.2.3. 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

תאריך: 11.07.2022

המידע והגנת הסייבר של מכבי . למען הסר ספק מאושר לחבר את השרתים או המחשבים לרשת האינטרנט כאשר מיושמות מערכות הגנה בניהם (כגון FW וכדומה).

2.2.4. לא יועבר ו/או ישמר מידע המכיל פרטים מזהים (ת.ז, שם ושם משפחה, טלפון, כתובת וכד')

2.2.5. 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.

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

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

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

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

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

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

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

2.2.10.2. הכניסה לתחנה תהיה באמצעות USER ID וסיסמא אישית .

2.2.10.3. אורך הסיסמא יהיה לפחות שבעה תווים.

2.2.10.4. הסיסמאות יוחלפו כל שלושה חודשים לפחות.

2.2.10.5. התחנה תינעל אוטומטית לאחר 5 שגיאות רצופות בהקשת הסיסמא.

2.2.10.6. בכל תחנה יותקן נועל מסך עם סיסמא שיופעל לאחר 20 דקות לכל היותר.

2.2.10.7. תותקן תכנת הגנה תקנית ומעודכנת כנגד וירוסים.

תאריך: 11.07.2022

2.2.10.8. מערכת ההפעלה המותקנת על התחנה מעודכנת בעדכוני האבטחה האחרונים שהופצו על

ידי היצרן.

2.2.11. 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.

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

גישה בלבד.

2.2.13. גיבויים יבוצעו בצורה מסודרת וישמרו במקום סגור ונעול עם גישה לאחראי על הגיבויים בלבד.

כמו כן על הספק לקיים נוהל שחזור תקופתי לגיבויים.

2.2.14. אין להעביר קלטות עם גיבויים של קבצים המכילים מידע של מכבי לגופים חיצוניים ללא ידוע

מראש.

2.2.15. כל מדיה מגנטית או אופטית או דוח המהווים תוצרי עיבוד מנתוני מכבי יאוחסנו בארון סגור וכן

יושמדו וייגרסו לאחר השימוש.

2.2.16. 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.

2.2.17. במידה וקיים שימוש בטכנולוגיה של רשת אלחוטית (wifi), הרשת תאובטח לכל הפחות ע"י שימוש

בהגדרות הבאות:

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

2.2.17.2. יבוצע שימוש בפרוטוקול WPA 2.

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

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

2.2.18.2. יוגדר לוג אירועים על השימוש בשירות.

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

תאריך: 11.07.2022

## 2.3. גישה לרשת ולמערכות מכבי -

2.3.1. 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:

2.3.2. 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.

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

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

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

2.3.6. 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.

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

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

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

## 2.4. שימוש באמצעי mobile ומחשבים ניידים:

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

תאריך: 11.07.2022

2.4.2. אמצעי ה-mobile ימצא בהשגחת עובד הספק בכל עת. במידה והעובד אינו לוקח את אמצעי

המחשוב הנייד עמו מסיבה כלשהי, עליו לנעול אותו במקום בטוח.

2.4.3. 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.

2.4.4. 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.

2.4.5. 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.

2.4.6. אין להעביר אמצעי גיבוי של קבצים המכילים מידע של מכבי לגופים חיצוניים ללא אישור מראש

ובכתב ממנהל אבטחת המידע והגנת הסייבר במכבי.

## 2.5. ארכיטקטורה

2.5.1. האתרים יהיו תחת Domain מכבי (כלומר URL של האתרים יהיו בDomain מכבי).

2.5.2. חל איסור עקב מגבלות טכנולוגיות לעבוד עם שירותים המבוססים על פרוטוקול Websocket.

במידת הצורך ניתן לפנות לאבטחת מידע והגנת הסייבר במכבי על מנת לאפיין פתרון חלופי.

2.5.3. במקרה של שליחת הודעות למבוטחים/עובדים - שליחת ה-SMS/ Whatsapp תבוצע אך ורק

למספרי הטלפון המעודכנים במכבי. זהות השולח תהיה מכבי שירותי בריאות.

2.5.4. במקרה של שליחת מיילים למבוטחים/עובדים - שליחת המיילים יועברו מכתובת של מכבי בלבד.

לצורך כך הספק מתחייב להעביר כתובות IP למכבי לצורך הגדרת SPF.

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

2.5.6. הספק יישם את הגדרות האבטחה הבאות:

2.5.6.1. האתרים המשמשים את הפתרון ימוגנו על ידי Web application firewall , ופתרון

.DDOS

תאריך: 11.07.2022

- 2.5.6.2. ממשק ניהול (מכל סוג) לא יהיה נגיש לכל כתובות האינטרנט, אלא יפתח ב FW רק לכתובות ספציפיות.
- 2.5.6.3. כל הנתונים ישמרו מחוץ לשרת ה WEB בשרת מסד הנתונים ייעודי .
- 2.5.6.4. שרת מסד הנתונים ישב בסגמנט ייעודי מופרד ב FW מסגמנט שרת ה WEB . סיגמנט זה יהיה חסום לגישה אל ומ – האינטרנט.
- 2.5.6.5. שירותי מכבי יפעלו בשרתים ייעודיים למכבי, בהם אינם שותפים גורמים נוספים. למען הסר ספק דרישה זו לכלל מרכיבי השירות.
- 2.5.6.6. עובדים פנימיים יזדהו למערכת על בסיס SSO (הזדהות מכבי)
- 2.5.7. בכל אתר / פלטפורמה שמזוהה בשם מכבי
- 2.5.7.1. תבוצע הפרדה בין שרתי מכבי לשרתי הספק ושרתי לקוחות נוספים. ההפרדה תבוצע לבאים: שרת זהויות, מסדי נתונים, שרתי WEB ואפליקציה.
- 2.5.7.2. שרת מסד הנתונים ושרת הזהויות, ישבו בסגמנט ייעודי מופרד ב FW מסגמנט שרת ה WEB. סיגמנט זה יהיה חסום לגישה אל ומ – האינטרנט.
- 2.5.7.3. תבוצע הפרדה בין סביבת הייצור לסביבת הפיתוח והבדיקות. ההפרדה תבוצע הן ברמת אפליקציה והן ברמת תשתיות (שרת ווב, שרת מסד נתונים וכו').
- 2.5.7.4. יוגדרו סיגמנטים ייעודיים עבור שרתי מכבי אשר יופרדו מבחינת תקשורת משאר שרתי הספק (הכוונה למערכות ההפעלה, ולא לברזלים המחזיקים את כלל השרתים הווירטואליים).
- 2.5.7.5. ההזדהות של עובדי מכבי לשירות תבוצע באמצעות SAML
- 2.5.7.6. באתרים יופעלו שירותי\מערכות הבקרה הבאים (השירותים\מערכות יופעלו במוד הגנה אקטיבית (חסימה) ולא במוד למידה):
- 2.5.7.6.1. FW – אפיון והגדרה של ה WAF באופן אקטיבי על בסיס התאמה לאתר האינטרנט.
- 2.5.7.6.2. IPS
- 2.5.7.6.3. ממשק הפלטפורמה ל- WAF של מכבי
- 2.5.7.6.4. Anti DOS\DDOS (להגנה ספציפית על אתרי מכבי).

תאריך: 11.07.2022

2.5.7.6.5. אנטי וירוס - האנטי וירוס יעודכן ברמה יומית.

2.5.7.6.6. 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.

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

## 2.6. ממשקי Web Service

2.6.1. כל ממשקי Web Services ינוהלו ויאובטחו לפי הנחיות מכבי שירותי בריאות ויכללו לכל הפחות:

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

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

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

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

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

## 2.7. הצפנה

2.7.1. דרישות תעודת הצפנה:

2.7.1.1. תעודת הספק תהיה מ issuer חיצוני ולא CA מקומי

2.7.1.2. אלגוריתם של התעודה תהיה sha256

2.7.1.3. התעודה תכיל CRL Distribution Points

2.7.2. דרישות לגבי ההצפנה:

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

תאריך: 11.07.2022

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

## 2.8. ניטור אירועים

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

2.8.2. לוג האירועים יוגדר על הבאים:

2.8.2.1. בכל מודול ומערכת שמאחסנת מידע של מכבי.

2.8.2.2. בכל רכיב בשרת: מערכת הפעלה, מסד הנתונים, וה-GUI.

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

2.8.3. לוג אירועים יופעל על האירועים הבאים:

2.8.3.1. כניסות למערכת – מוצלחות או כישלונות.

2.8.3.2. כל גישה לנתונים, כולל קריאה בלבד.

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

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

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

2.8.4. רישום כל אירוע יכלול את הערכים הבאים:

2.8.4.1. מועד ביצוע הפעולה.

2.8.4.2. שם משתמש מבצע הפעולה.

2.8.4.3. כתובת מקור.

2.8.4.4. סוג ה – Client.

2.8.4.5. שם הפעולה.

2.8.4.6. סטטוס – הצלחה\כישלון.

2.8.4.7. תיאור הפעולה.

## 2.9. פיתוח

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

2.9.1. האתר יפותח בסטנדרט פיתוח מאובטח – OWASP-Top 10

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

אחרים.

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

תאריך: 11.07.2022

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

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

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

2.9.7. חל איסור לבצע שימוש במידע חסוי/חסי/ ביותר/ מידע אישי מזהה Test Data בתהליכי QA ופיתוח. לתהליכים אלו יש להשתמש בData אנונימי או בData רנדומלי בלבד

2.9.8. חריגה מאופשרת באישור מראש על ידי מכבי שירותי בריאות

## 2.10. אבטחת מידע בענן:

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

2.10.2. ספק הענן יהיה ב- EU Region בלבד

2.10.3. ספק שירותי הענן יגדיר איש קשר לנושאי אבטחת מידע(בקורות ואירועים).

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

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

2.10.6. 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.

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

2.10.8. 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.

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

תאריך: 11.07.2022

2.10.10. 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 27799, חוק הגנת הפרטיות.

#### 2.10.11. ניהול זהויות והרשאות בענן:

- 2.10.11.1. גישה לשירות (הן ניהולית והן מצד לקוח) תבצע במשתמש אישי בלבד.
- 2.10.11.2. בשירות יוגדר פרופיל ההזדהות בהתאם למדיניות הארגון (חוק סיסמה, נעילה לאחר כניסות שגויות, ניתוק לאחר אי שימוש וכו').
- 2.10.11.3. ההזדהות תבוצע באמצעות SAML בלבד. על הספק לחסום כל אפשרויות הזדהות אחרות.
- 2.10.11.4. ההזדהות תתאפשר מכתובות IP של מכבי בלבד.

#### 2.10.12. אחסון מידע

- 2.10.12.1. נתוני מכבי ימחקו מהתקני המחשוב בהם משתמש הספק לאחר סיום השימוש בהם או בתום השירות, הראשון מבניהם.
- 2.10.12.2. על פי צורך, תתאפשר לארגון יכולת למחיקה מוחלטת של המידע מהשירות.

#### 2.10.13. הצפנת המידע

- 2.10.13.1. נתונים המוגדרים כרגישים (ובכל מקרה במידע רפואי של לקוחות) יוצפנו באחסון.
- 2.10.13.2. ההצפנה תבוצע בהתאם לסטנדרטים המקובלים בשוק.
- 2.10.13.3. מפתחות ההצפנה יישמרו באופן בלעדי בידי הארגון במידת האפשר.

#### 2.10.14. ניטור אירועים

- 2.10.14.1. ניטור אירועים על פי המוגדר בסעיף ניטור אירועים

#### 2.10.15. העברת מידע

- 2.10.15.1. העברת המידע תבוצע בתווך מזוהה ומוצפן.