

בקשה לקבלת מידע (RFI)

עבור עיצוב וייצור עמדת שירותי משרד בשירות מרחוק / שירות עצמי (להלן –

"הבקשה")

1. כללי

1.1. מכבי שירותי בריאות (להלן – "מכבי") מעוניינת לקבל מידע באשר לספקים פוטנציאליים המסוגלים לעצב, לייצר ולתפעל (כולל תחזוקה שוטפת) "עמדת שירותי משרד במודל מתן שירות מרחוק ובמודל של שירות עצמי".

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 עד לתאריך 18.05.2023.

1.3. על המשיב העונה להיות בעל ניסיון קודם בייצור עמדות לשירות עצמי על פי הפירוט המוצג במסמך זה.

1.4. רק פניות מתאימות תענינה. רק לאחר בחינת הפניות המתאימות יועבר אפיון מלא לעמדה לספקים הרלוונטיים, בכפוף לשיקול דעתה של מכבי. כמפורט בסעיף 3 לבקשה.

1.5. 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 הליך רכש / מכרז בנושא. הבקשה נועדה לקבלת מידע בלבד ובעקבותיה תשקול מכבי את המשך פעולותיה בהתאם לשיקולים מקצועיים וענייניים.

1.6. מכבי שומרת לעצמה את הזכות לקיים מפגש אליו יוזמנו המשיבים שנטלו חלק בשלב זה של הפנייה לקבלת מידע או את חלקם, והכל לפי שיקול דעתה הבלעדי של מכבי.

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, למוסר המידע לא תהיינה טענות בדבר זכויות יוצרים מכל מין וסוג שהם.

1.8. מכבי שומרת לעצמה את הזכות לפרסם פנייה נוספת ו/או לפרסם בקשה להצעות מחיר ו/או לא להתקשר בהסכם כלשהו עם מי מהפונים. אם יתקיים הליך רכש נוסף בעתיד, תהא מכבי רשאית לשנות או להוסיף תנאים ודרישות מעבר לאחר 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 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.

2. רקע

- 2.1. מכבי שירותי בריאות מעוניינת לקבל מידע באשר לספקים פוטנציאליים לטובת אספקת עמדת שירותי משרד אשר תשרת את חברי מכבי המעוניינים לקבל שירותי משרד מנציגת שירות מרחוק ובמקביל תאפשר לקבל שירותים בשרות עצמי מלא או חלקי.
- 2.2. העמדה תכלול מבנה וציוד טכני לצורך תפעול מערכות המחשוב על ידי נציגי שירות מרחוק וציוד קצה ייעודי לשרות עצמי מלא ועמדת שליטה לנציג/ה המרוחקת.
- 2.3. מהות העמדה לאפשר קבלת שירות מרחוק/עצמי לחברי מכבי שאינם דיגיטליים, מבוגרים, בעלי מוגבלויות טכניות או מוגבלויות שפה אשר מגיעים פיזית לקבל שירותי משרד פרונטאלית במכבי.
- 2.4. העמדה מיועדת לאפשר חווית משתמש זהה לזו המסופקת פרונטאלית.

3. מפרט ודרישות מהמערכת

- הקמת עמדת קבלת קהל העומדת בתקני נגישות, וכוללת ציוד טכני לצורך תפעול של נציגת מכבי מרחוק וגם לחילופין תאפשר קבלת שירותים בשרות עצמי מלא או חלקי בדומה לשירות הניתן פיזית.
- המציע מתבקש לספק מענה על כלל סעיפי הבקשה.
- **על המציע לעמוד בדרישות אבטחת מידע כמפורט בנספח א' למסמך זה, ולענות על שאלון אבטחת מידע כמפורט בנספח ב'.**
- הצעת המציע תיבדק, במידת הצורך תיכלל גם שיחה/פגישה עם גורם מקצועי, בכפוף לשיקול דעתה של מכבי.
- במידה וההצעה תימצא מתאימה, המציע יוזמן לקבל אפיון מדויק ומפורט של עמדת השירות העצמי.
- בהמשך, על המציע יהיה להציג תכנון מפורט לעמדת "prototype" ישימה.

3.1. דרישות מהמערכת

- 3.1.1. על המערכת להציג במסך לחברים פרוט כתוב וויזואלי של הפעולות הנדרשות לבצע וזאת בצורה ברורה ופשוטה כך שניתן יהיה לצורך את השירות ללא צורך בעזרה פיזית של נציג שירות.
- 3.1.2. על הספק לבנות שיטות עבודה מובנות מצד נציגת השרות כך שיהיו עד כמה שניתן קצרות, אוטומטיות וברורות ולפתח בקורות המונעות טעויות אנוש מצד הנציגה.
- 3.1.3. המערכת נדרשת להוציא דוחות בקרה יומיים על כל נתוני ההפקדה הן בשקים, הן במזומן והן כרטיסי אשראי.

3.2. דרישות מהעמדה

- 3.2.1. העמדה תעמוד בתקני נגישות ישראל.
- 3.2.2. העמדה תכלול נקודות תקשורת מידע.
- 3.2.3. העמדה תאפשר לספק שירותים סטנדרטים של משרד מכבי לכל חברי מכבי.
- 3.2.4. הדו שיח עם נציג השרות מרחוק יתאפשר באמצעות שיחת ווידאו על גבי מסך דיגיטלי.

3.2.5. השירותים הטכנולוגיים יאפשרו:

- לשלם במזומן
- לקבל עודף - שטרות ומטבעות
- לשלם בכרטיס אשראי העומד בתקני EMV
- אפשרות לשלם בהמחאות שיקים עם יכולת תפעול והדפסה של הנציג מרחוק על חזית ההמחאות
- יכולת הדפסת מסמכים מרחוק
- סריקת מסמכים וחתימתם
- מתן אפשרות להפקדת מסמכים פיזיים לתוך כספת וסריקה דיגיטלית משולבת של מסמכים אלו
- אפשרות לקריאה וסריקת המחאות ושוברים
- לכל השירותים הטכניים בסניף נדרש פתרון להפעלה מרחוק ללא התערבות אדם בסניף.

3.3. חומרה נדרשת

* המערכת חייבת להיות מותאמת לטובת מתן שרות באופן מלא ושוטף. לכן יש לתת גיבוי לפונקציות העיקריות באירועי כשל וזאת עד להגעת טכנאי שרות (להלן "גיבוי").

- 3.3.1. סורק שיקים ייעודי המתאים לשרות עצמי ומערכת גיבוי חומרתית אלטרנטיבית כגיבוי לרכיב.
- 3.3.2. סורק שוברים ייעודי המתאים לשרות עצמי ומערכת גיבוי חומרתית אלטרנטיבית כגיבוי לרכיב.
- 3.3.3. מערכת אוטומטית לתשלום בשטרות מזומנים והחזרת עודף בכל סוגי השטרות הישראלים (20,50,100,200) ומערכת גיבוי חומרתית אלטרנטיבית כגיבוי.

- המערכת תתמוך בתא הזנה של עד X שטרות מעורבים בהפקדה אחת (בפעולת תשלום)
- המערכת תתמוך בהחזרת השטרות האוטנטיים שהופקדו באם הלקוח התחרט.
- זיהוי ותיעוד של מספרים סידוריים של השטרות המופקדים.
- 3.3.4. מסך תצוגה HD בגודל מינימאלי של 21 אינץ' עבור שידורי ווידאו ומערכת גיבוי חומרתית אלטרנטיבית כגיבוי לרכיב.
- 3.3.5. מסך משתמש MultiTouch HD בגודל מינימאלי של 21 אינץ' ומערכת גיבוי חומרתית אלטרנטיבית כגיבוי לרכיב.
- 3.3.6. מצלמות ווידאו HD לצורך שיחה ותיעוד
- 3.3.7. מדפסת שיקים ייעודית למילוי פרטי השיק המתאים לשירות עצמי:
 - מדפסת השיקים לא תאפשר הדפסה טעויות הדפסה בשרות עצמי בגין:
 - הזנה לא נכונה של כיוון השיק
 - הדפסה חוזרת על שיק מודפס
- 3.3.8. יחידת סריקה הכוללת מודול לגריפה עד X מסמכים משודכים בגריפה אחת ויכולת אחסנתם בכספת פנימית בתום הגריפה:

- יחידת הסריקה תאפשר סריקה מסמכים מנייר, ממסכי מכשירים ניידים, תעודות זהות, דרכונים, מקבץ מסמכים משודכים.
 - יחידת הסריקה תאפשר לסרוק ריבוי מסמכים לתא הפקדה ותאפשר החזרתם ללקוח בגין חרטה.
 - יחידת הסריקה תכלול תריס פתח כניסה ויציאת מסמכים. התריס יישלט לפתיחה וסגירה מרחוק ע"י נציג השרות כך שלא ניתן יהיה לגורם חיצוני אפשרות לשלוף מסמכים מהחבילה לאחר סריקתם במערכת.
 - יחידת הסריקה תתמוך בסריקת מסמכים צבעונית, קורא ברקוד דו מימד ותעודות זיהוי עם יכולת הגדלה אופטית של המסמך הנסרק.
- 3.3.9.** קורא כרטיסי אשראי עם מקלדת מוצפת התומך בתקן EMV ומערכת גיבוי חומרתית אלטרנטיבית כגיבוי לרכיב.
- 3.3.10.** מסך ניהול שרות אחורי MultiTouch
- 3.3.11.** מתקן למתן עודף במטבעות 4 סוגים שונים ב קיבולת X מטבעות מינימום לעריך
- 3.3.12.** שפורפרת טלפון בעלת יכולת ניתוק אוטומטי של מערכות השמע ומעבר לשיחה דיסקרטית
- 3.3.13.** המערכת תאפשר יכולת חתימה דיגיטלית על מסמכים.
- 3.3.14.** תשתית לזיהוי חברי מכבי דיגיטלית ולא דיגיטלית.
- 3.3.15.** מצלמת HD לצילום החבר
- 3.3.16.** מדפסת לייזר הכוללת מינימום 2 מגרות של X דפים כל אחת לתמיכה בסוגי נייר שונים, ומערכת גיבוי אלטרנטיבית כגיבוי לרכיב.

3.4. דרישות חומרה כלליות

- 3.4.1.** לכל רכיב בעמדה יהיה תיאור במילים, מספר רכיב ומערכת תאורה אקטיבית שתפעל בעת הפניית החבר לרכיב הנדרש.
- 3.4.2.** שירותי התחזוקה של המערכת יינתנו מחדר השרות האחורי כך שלא ימנעו עבודה שוטפת של הסניף.
- 3.4.3.** החומרה תתמוך בתקני נגישות ישראל.
- 3.4.4.** חיבור ציודים ב-USB בלבד ללא צורך במתאמים

3.5. דרישות המערכות:

3.5.1. מערכת ווידאו

- מערכת ווידאו דו סיטרית לניהול שיחה בין נציג שרות לקוחות ללקוח
- אפשרות הוספת משתתף לוועידת ווידאו
- אפשרות העברת ניהול שיחה לנציג אחר
- אפשרות ניהול תורים, כך שחבר שמגיע למרכז הרפואי יופנה אוטומטית לנציג פנוי

- אפשרות פנייה לנציג שרות תוך כדי תהליך שרות עצמי ואפשרות הנציג להשתלט על המערכת ולסיים את הפעולה
- מערכת מעקב בזמן אמת של פעולות החבר מול המכונה לצורך הנחייה מדויקת

3.5.2. מערכת סריקה

- אפשרות ארכוב מסמכים נסרקים ולאגדם על פי בחירה לקובץ אחד מאורכב
- אפשרות הצגת המסמך/מסך הנסרק לפני ארכוב
- אפשרות הגדלה דיגיטלית של המסמך הנסרק לצורך זיהוי ברור עבור הנציג מרחוק
- אפשרות הפקדת מסמכים לתוך כספת מסמכים נעולה
- אפשרות סריקת ברקוד דו מימד ממסמך/מסך

3.5.3. תשלום מזומן

- אפשרות תשלום בשטרות מזומנים והחזרת עודף בכל סוגי השטרות הישראליים (20,50,100,200)
- אפשרות מתן עודף בכל סוגי השטרות וב – 4 סוגי מטבעות.
- אפשרות החזרת השטרות לחבר (הנחייה מרחוק במסך הלקוח)
- אפשרות הזנה של עד X שטרות מעורבים בהפקדה אחת (בפעולת תשלום)
- התייחסות אוטומטית במתן עודף לרמת המזומנים בקופות, כך שכמות הכסף בקופות תהיה תמיד מאוזנת

3.5.4. תשלום בשיקים

- אפשרות קבלת שיקים בשירות עצמי ללא התערבות נציג שירות תוך ביצוע בקורות של פרוט השיק, סכום, תאריך, מוטב וחתימה והתאמתו לדרישות התשלום.
- בסוף תהליך התשלום, מונפקת לחבר קבלה, אי לכך צריך לוודא שכול הפרטים מתאימים.
- נדרשת אפשרות מתן אופציה לפריסת תשלומים בשירות עצמי

3.5.5. תשלום בכרטיסי אשראי

- נדרשת אפשרות תשלום בכרטיס אשראי מאובטח
- כל פעולה מחוייבת להיות עם ליווי מונחה וויזואלי על מסך המשתמש של המערכת הדיגיטלית
- בסינכרון מלא עם פעולות בפועל, כגון הוראות הכנסת כרטיס, הקשת הקוד, זיהוי הוצאת הכרטיס ועוד...

3.6. בקרה

3.6.1. המערכת תדווח על תקלות בכל רכיבי המערכת למערכת שליטה ובקרה

3.6.2. המערכת תדווח על רמות מלאי של רכיבי המערכת לרבות מדפסת, מלאי מזומנים, שיקים ומסמכים מופקדים

3.6.3. המערכת תאפשר השבתה, איתחול מחדש, ושדרוג הפצת תוכנה מרחוק

3.6.4. המערכת תדווח על תקלות ברכיבי פתיחה וסגירת הדלתות ותתריע באם הדלתות פתוחות או סגורות בזמני הפתיחה של הסניף המוגדרים מראש.

3.6.5. כמו כן תדווח לוג מלא על שעות פתיחה וסגירה של דלתות הסניף ע"י מורשים.

3.7. תשתיות

- מ"ה - Windows 10 גרסה אחרונה ומעלה
- מסמכי Adobe Acrobat Reader DC – PDF גרסה אחרונה ומעלה
- דפדפן – Chrome ו-Edge
- מסמכי Office במידה ונדרש – תמיכה בגרסת LTSC 365 ללא צורך ברישוי פר משתמש
- עבודה עם Windows Defender Anti-Virus (האנטי וירוס הארגוני)
- עדכוני אבטחה יבוצעו על ידי מכבי.

4. ממליצים

לקוחות מרכזיים עבורם בוצע עיצוב וייצור עמדה בהתאמה אישית

לקוח	ענף	תאור העמדה	איש קשר	טלפון

5. הערכת עלויות

הערכת מחיר כוללת לרכש של עמדת שירות אחת (כולל: עיצוב, ייצור, הובלה, התקנה, תחזוקה):

ש"ח, לפני מע"מ, לעמדה. _____

זמן משוער נדרש לאספקת עמדת שירות ותחילת עבודה: _____

*המחירים אינם כוללים מע"מ

6. מסמכים שיש לצרף לבקשה:

- המלצות
- פרוספקטים
- כל מידע רלוונטי אחר (כגון: ניסיון בתכנון, הטמעה ותפעול העמדה)

נספח א'

הנחיות לדרישות מדיניות אבטחת מידע בפרויקט קיוסק רפואי:

1. רקע

מכבי שירותי בריאות מקדמת פתרון שירותי משרד היברידיים ע"י עמדות קיוסק שמשלבות שירותים פרונטליים, טלפוניים ושירות עצמי.

2. מטרה

להעביר הנחיות ליישום הטמעה ושימוש מאובטח בעמדות הקיוסק תוך שמירה על מידע רגיש.

3. הזדהות לקוחות

3.1 כאשר מבוטח מזדהה מול עמדת הקיוסק, ניתן לבצע הזדהות חזקה באמצעות אחד מהאפשרויות הבאות:

3.1.1 שימוש בכרטיס דיגיטלי בטלפון + OTP

3.1.2 הזדהות באמצעות ת.ז. + תאריך לידה + שליחת קוד OTP לטלפון הלקוח אשר מופיע במערכת (הלקוח אינו נדרש להזין את הטלפון).

3.1.3 העברת כרטיס מכבי + OTP

3.2 המערכת תנתק את הלקוח במידה ולא הייתה תגובה לאחר פרק זמן של 30 שניות.

3.3 למערכת יהיה כפתור ניתוק לקוח במידה והלקוח ירצה להתנתק באופן יזום.

4. ארכיטקטורה המערכת

4.1 שרתים ועמדות קצה לפרויקט – כלל השרתים והעמדות יהיו חברות בדומיין קיוסקים (יש ליצור כזה) ויקבלו פוליסי מנוהל לשמירת מדיניות אבטחת המידע.

4.2 סגמנטציה – הפרדת רשתות – לא תאפשר גישה חופשית בין שרתים ועמדות הקצה של המערכת וגישה לשרתי BE מסדי נתונים וכו' תאפשר למענה הצורך בלבד לשירותים הנדרשים בלבד.

4.3 גישה מה FE ל BE במערכת תעבור דרך FW.

4.4 כל תעבורה אשר נשלחת מתקבלת מעמדת הקיוסק נדרשת להיות מוצפנת ע"פ הסטנדרט בשוק (TLS 1.2 ומעלה).

4.5 תהליך ההתקשרות מול מערכות פנימיות יתבצע ע"י Mutual Authentication מבוסס סרטיפיקט.

4.6 ממשקים ינוהלו דרך רכיב API-GW.

4.7 יש להשתמש ב- Active Directory ייעודי עבור עמדות קיוסק, במקום להשתמש ב AD הארגוני.

5. מאפייני מערכת ההפעלה

5.1 מערכת ההפעלה תעלה עם Golden image בכל הפעלה של הקיוסק מחדש.

5.2 התוכנה המוצגת בעמדת הקיוסק נדרשת להיות במצב מוקשח מלא, ללא יכולת יציאה ממצב זה (גם לא בשימוש בכפתורים מיוחדים במקלדת).

5.3 יש לוודא עם הספק שאין סיסמאות Hard Coded במערכת.

5.4 אחת לרבעון יש לבצע תהליך עדכון תוכנה של מערכות ההפעלה ושל הכלים במערכת.

5.5 נדרשת יכולת התממשקות אל מול Active Directory.

5.5.1 התוכנה תעבוד עם משתמש דומיניא אפליקטיבי ייעודי עם הרשאות מינימליות רק להפעלת

התוכנה (יש לעבוד על פי עקרון Least Privileges).

5.6 הזדהות המערכת אל מול API

5.6.1 יש לממש מערכת ניהול מרכזית לקיוסקים

5.6.2 שימוש ב-API יתבצע מול רכיב הניהול המרכזי (middleware) לקיוסקים

5.6.2.1 middleware יבצע זיהוי למשתמש הדומיננטי, ולאחר ולידציה הרכיב המרכזי ישלח ויחזיר

את הנתונים ל-API-GW.

5.6.2.2 לחילופין, ה middleware יבצע זיהוי באמצעות תעודה שהונפקה לתחנה הקצה, ולאחר

ולידציה הרכיב המרכזי ישלח ויחזיר את הנתונים ל-DataPower.

5.6.2.3 ההזדהות בין Middleware ל-API-GW תהיה mutual Authentication certificate base.

6. הקשחת עמדת קיוסק

6.1 נדרשת התקנת DLP על המכונה אשר חיבור רכיבי קצה מאושרת על ידי רשימה לבנה.

6.2 נדרשת התקנת מערכת EDR על עמדות הקצה.

6.3 שירותים שלא הכרחיים בעמדת הקיוסק לטובת הפרויקט/המערכת ינוטרלו.

6.4 עמדת הקיוסק תבצע הזדהות מול NAC באמצעות סרטיפיקט (certificate) (802.1x).

6.5 יש לבצע הקשחה מלאה לעמדת הקיוסק כך שלא יהיה ניתן לצאת מגבולות התוכנה כאשר היא פועלת

או בעת אתחול עמדת הקיוסק.

6.6 אין לשמור מידע רגיש בעמדת הקיוסק.

6.7 החרגת AV תעשה ברמת השירות (Service) ולא ברמת תיקייה.

6.8 מערכת ההפעלה המותקנת על עמדת הקיוסק נדרשת להיות Image מכבי ייעודי לעמדות קיוסק.

6.9 הזדהות רכיבי תקשורת מול מערכת ה-NAC נדרשים בזיהוי חד חד ערכי.

7. שרשרת האספקה – גישת ספקים

7.1 ספקים יתחברו למערכת ולסביבת מכבי פנימיות דרך מערכת PIM לצורך תמיכה ושירות.

7.2 העברת קבצים בין הספק למכבי תיעשה ע"י מערכת כספות.

7.3 יש לבצע בדיקת חדירות לפני העלאה לייצור.

7.4 יש לבצע בדיקת חדירות לעמדת הקצה בכל שינוי גרסה.

7.5 אין לשמור או להתקין תוכנת השתלטות מרחוק על המכונה.

8. פיתוח מאובטח

8.1 סביבות הפיתוח יהיו פנימיות בלבד. סביבות אלו לא יהיו נגישות באופן ישיר מהאינטרנט. (בין אם

הפיתוח ייעשה בחצרות מכבי או בחצרות הספק)

8.2 לפני העלאת גרסה לייצור יש לבצע מבדקי חקירות, אין להעלות גרסה לייצור עם ממצאים

מהותיים. (גבוהה או קריטית)

8.3 שרתי ה-DB יהיו מופרדים תקשורתית משאר הרשת והגישה אליהם תאופשר אך ורק בפרוטוקולים

הנדרשים. שירותים אלו לא יהיו בסביבת תקשורת בה קיימת גישה (גם לשרת אחר) מרשת האינטרנט

(כלומר SDMZ לכל הפחות).

8.4 כל שינוי במערכת מחויב לעבור תהליך ניהול שינויים והעלאה לייצור שילול שלב פיתוח, שלב QA ושלב

עליה לייצור.

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

8.6 הספק ינהל מעקב אחר רכיבי הקוד בהם הוא עושה שימוש, במידה ויש התרעת אבטחת מידע על אחד הרכיבים בהם נעשה שימוש בקוד על הספק להוציא עדכון לא יאחר משבועיים לאחר קבלת ההתראה.

8.7 נדרש לעגן תכנית patch management למערכת בסביבת הענן ובסביבת מכבי הממפה את הכלים והתוכנות בהן נעשה שימוש.

8.8 זיהוי פגיעות בכלי או בתוכנה בה המערכת עושה שימוש יטופל בתוך שבוע ימים מגילוי הפגיעות.

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

8.9.1 לעבוד עם הכלים הקיימים ברשת מכבי.

8.9.2 לעבוד בתשתיות ה DevOps הקיימות של מכבי.

8.9.3 להורדת כלים נוספים יש לקבל אישור אבטחת מידע.

9. ניטור אירועים

9.1 יוגדר ויופעל לוג אירועים מלא על כלל האירועים בכלל מרכיבי המערכת. וכן בכל שרתי המערכת המיועדים למכבי.

9.2 תבוצע אינטגרציה בן לוגי האירועים למערכת ה SIEM של מכבי (QRADAR). אינטגרציה זו תבוצע ע"י מכבי ובסיוע מלא של הספק.

9.3 לוג אירועים יבוצע על המרכיבים הבאים לכל הפחות:

9.3.1 כל מודול ומערכת המאחסנת מידע של מכבי.

9.3.2 כל רכיב בשרת: מערכת הפעלה, מסד הנתונים, וה- GUI.

9.3.3 כל רכיב במערכת: אתר משתמשים, back office וכו'.

9.4 לוג אירועים יופעל על האירועים הבאים לכל הפחות:

9.4.1 כניסות למערכת – מוצלחות או כישלונות.

9.4.2 כל גישה לנתונים, כולל קריאה בלבד.

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

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

9.4.5 שינוי הגדרות מערכת. כולל שינוי במערכת המשתמשים וההרשאות.

9.5 רישום כל אירוע יכלול את הערכים הבאים:

9.5.1 מועד ביצוע הפעולה.

9.5.2 שם משתמש מבצע הפעולה.

9.5.3 כתובת מקור.

9.5.4 כתובת יעד (במידה ומצוין)

9.5.5 סוג ה- Client.

9.5.6 שם הפעולה.

9.5.7 סטטוס – הצלחה\כישלון.

9.5.8 תיאור הפעולה.

9.5.9 יש לאפיין לוגים ייעודים בהתאם לשימוש המערכת ולשירותים שהיא עונה עליהן כדי לקבל תיאור מלא של הפעולה והשירות. – נדרש אפיון ייעודי לקבלת הלוגים טרם חיבור המערכת מול הגורם המפתח.

9.5.10 גישת מערכת ה – SIEM למערכת ולעמדת הקיוסק-

9.5.11 נדרש לקבל מהמערכת ומעמדת הקיוסק Syslog לטובת האינטגרציה.

נספח ב'

פרק אבטחת מידע לשאלון RFI:

מטרת השאלון הינה לתת למחלקת אבטחת מידע יכולת להעריך האם המוצר נותן מענה לדרישות אבטחת המידע הבסיסיות של מכבי שירותי בריאות. השאלון לא מחליף את הנחיות אבטחת המידע ליישום והטמעת המוצר אלא נוצר כדי לתת למחלקת אבטחת המידע מושג ראשוני אודות מודעות אבטחת המידע של הספק ומענה לצרכי אבטחת מידע בקרב המוצר.

1. היכרות עם המוצר \ מערכת \ פתרון.

1.1. אנא תאר אודות המוצר והמענה לצורך לו הוא נותן מענה:

2. שאלות ודרישות כלליות:

- a. האם המערכת המוצעת כוללת חומרה או חומרה ותוכנה? אנא פרט.
- b. האם הטמעת המערכת היא מקומית (on-prem), שירות ענן (SAAS, PAAS), IAAS או היברידי? אנא פרט.
- i. במידה והמערכת מותקנת מקומית על הספר לעמוד בדרישות אבטחת המידע ליישום ב-On-Prem
- ii. במידה והמערכת נמצאת הענן על הספק לעמוד בדרישות אבטחת מידע לענן ובוועדת ענן.
- c. על הספק, לספק ארכיטקטורת פתרון ברמת HLD לטובת הפתרון המוצע.

3. הזדהות

1. היכן מתבצע הליך הזיהוי ולמול איזה מערכות?
 - a. במידה וההזדהות מבוצעת למול מנגנון הזדהות של הספק, אנא ספק פירוט על המנגנון ואמצעי הזיהוי ואיזה בקורות מפצות קיימות בתהליך.

2. האם המערכת כוללת תהליך זיהוי חזק?

- a. תהליך זיהוי חזק כולל בתוכו הזדהות דו-שלבית
- b. במידה והנך מיישם זיהוי דו שלבי, אנא פרט ובמידה לא, אנא ציין חלופות.

3. גישת משתמשים למערכת

- a. האם הגישה למערכת נעשית באופן מוצפן? במידה וכן פרט.
- 3.1 ניהול סשנים במערכת
- b. כיצד מבוצע ניהול הסשן? אנא פרט.
- c. כמה זמן הסשן פעיל?
- d. האם מתקיים תהליך Logout אוטומטי?
- e. האם נשמרים מזהים ברמת התחנה, האתר או האפליקציה?
- i. במידה וכן, האם מאוחסנים בתצורה מוצפנת, במידה ולא, אנא פרט.

3.2 טוקן גישה מאובטח

- a. האם גישה למערכת מותנית בהנפקת טוקן מאובטח למשתמש?
- b. האם נעשה שימוש ב – session ID רנדומלי?
- c. האם נעשה שימוש בטוקן המכיל חתימה הכולל גם TTL.

ממשקים

- 4. אנא מנה את ממשקי המערכת וסוגם.
- 4.1 מהו תהליך זיהוי הממשקים?
- 4.2 מהו תהליך העברת המידע בממשקים?
- 4.3 כיצד מבוצעת ההגנה על הממשקים במערכת לרבות ממשקים מבוססים API או כל ממשק אחר?
- 4.4 האם הממשקים כוללים ניטור?

5 אחסון

- 5.1 האם המערכת שומרת נתונים?
- 5.2 היכן הנתונים נשמרים?
- 5.3 האם המידע אשר נשמר מוצפן?
- 5.4 פרט כיצד מתבצעת ההצפנה.

6 עמידה בתקני אבטחת מידע

- 6.1 האם המערכת עומדת בתקן GDPR.
- 6.2 האם המערכת עומדת בתקן HIPPA.
- 6.3 האם הספק עומד בתקן אבטחת מידע ISO 27001\27799.

7 סיווג מידע

- 7.1 האם המערכת מעבדת מידע אישי מזוהה?
- 7.2 האם המערכת מעבדת מידע רפואי?
- 7.3 האם המערכת מעבדת מידע עסקי רגיש?
- 7.4 האם המערכת מעבדת רפואי לא מזוהה?

8 גישה לאינטרנט

- 8.1 האם המערכת דורשת גישה לאינטרנט? במידה וכן, לאיזה צורך?

9 בקורות מפצות והגנת סייבר

- 9.1 האם הפתרון משלב מנגנוני אבטחת מידע? אנא פרט במידה וכן.