

בקשה לקבלת מידע (RFI) בנושא מערכת ניהול, הפקת דוחות וממשק נציג וחייגן למערכת AVAYA

(להלן "הבקשה")

1. כללי

- 1.1 מכבי שירותי בריאות (להלן – "מכבי") מעוניינת לקבל מידע למערכת ניהול, הפקת דוחות וממשק נציג וחייגן למערכת AVAYA (להלן – "המוצרים והשירותים"), כמפורט בבקשה.
- 1.2 את ההצעות יש למלא על גבי טופס ההצעה הבקשה המצורף ולשלוח אל מאור שרגא לדואר אלקטרוני shraga_ma@mac.org.il עד תאריך 21/7/2024.
- 1.3 פרסום הבקשה למידע אינו מבטל את זכותה של מכבי להמשיך התקשרויות קודמות בהתאם לשיקול דעתה הבלעדי, עם מציע, ואין בעובדה שמציע התייחס במסגרת בקשה זו על מנת לבטל ו/או לשנות ו/או לגרוע מזכויות מכבי בהתאם להסכמים קודמים עימו, 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. 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 אם יתקיים הליך מכרז בעתיד, תהא מכבי רשאית לשנות או להוסיף תנאים ודרישות מעבר למפורט בבקשה זו – הכול לפי שיקול דעתה המקצועי הבלעדי ובהתאם לצרכיה כפי שיהיו מעת לעת.
- 1.6 במידת הצורך, המציע ימציא למכבי מסמכים נוספים או שייפגש עם גורמים במכבי לשם בחינת עמידתו בתנאי סף או במפרט המבוקש.
- 1.7 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.

2. תיאור כללי של הדרישות המקצועיות לנשוא הבקשה

2.1 רקע לבקשה:

- מכבי מעוניינת לקבל מידע עבור מערכת הכוללת ממשקי ניהול, דוחות וממשק נציג למערכת AVAYA מסוג AACC המשרתת את מוקדי מכבי.
- המערכת תותקן ב-On Premise של מכבי.
- מפרט הדרישות בטופס ההצעה להלן.

2.2 מצב קיים:

- 2.3 מערכת מוקדים AVAYA : CONTACT CENTRE – מרכזיית CM ותוכנת מוקד מדגם AACC. כ-900 נציגים פועלים במשמרת (בוזמנית), סה"כ 2,500 משתמשים (NAMED).

3. טופס ההצעה

3.1. פרטי המציע:

התאגיד המציע:

יצרן:

שם המוצר:

ותק הטכנולוגיה בארץ/בעולם:

תיאור הדרישה	קיים (כן/לא)	התייחסות מפורטת
לפרט את הסמכות היצרן AVAYA לרלוונטיות למימוש המערכת המוצעת ואופן התמיכה של היצרן בפתרון המוצע		
המערכת המוצעת על ידי המציע מיושמת ומופעלת בלפחות 3 מוקדים עם לפחות 250 נציגים. על גבי מערכות Avaya - מרכזיית CM ותוכנת מוקד מדגם AACC		
המציע הינו אינטגרטור מורשה של היצרן חברת AVAYA בדרגת Sapphire לפחות		
למציע ניסיון מוכח בישראל ב-3 השנים האחרונות לפחות, באספקת ובהתקנת המערכת המוצעת		
לפרט את היקף עובדים, פריסה בארץ, תחומי התמחות עיקריים וכמות מיישמים שתומכים מטעמו במערכת המוצעת		
המציע מספק שירותי תמיכה שירותי התמיכה 24/7 בטלפון ובמייל		
המציע מסוגל לספק בעצמו את המערכת והשירותים הנדרשים לרבות פיתוחים, התאמות, תמיכה וכד'		
הערכת משמעות מימוש המערכת והטמעתה במכבי – לו"ז, משאבים נדרשים ממכבי (כולל פיתוחים מחישוביים) וכד'		
ממשק הנציג יתמוך לפחות בשפות עברית, אנגלית		

3.2. לקוחות מרכזיים למוצר/שירות:

חברה	ותק במכירת המוצר/שירות	איש קשר	טלפון

3.3. התייחסות למפרט :

ממשק נציג מתקדם :

תיאור הדרישה	קיים (כן/לא)	התייחסות מפורטת
תמיכה ואינטגרציה למערכת AVAYA מדגם AACC		
התמיכה ואינטגרציה למערכות VDI		
תיאור אופן ביצוע הלוגין (Login) למערכת		
תמיכה בעבודה של נציגים ואחיות מהבית		
המערכת תכלול יכולת הקפצת מסך של מערכת ה-CRM של מכבי אינטגרציה למערכת CRM		
המערכת תאפשר הצגה של סוג הקמפיין והתמחות ממנו השיחה הגיעה, כשיחה נכנסת/יוצאת		
ממשק הנציג יתמוך בעבודה עם Soft Phone של חברת AVAYA להפעלת כל הפונקציות הטלפוניות הקיימת		
סרגל הנציג יכלול את התכונות הבאות: התייעצות, ועידה, מענה לשיחה, העברה, החזק, חיוג ידני, חיוג חוזר, השתקה		
הממשק יכלול הצגת הסטאטוס הנוכחי והזמן בסטאטוס, של עבודת ניירת והפסקות שונות.		
ממשק הנציג יתמוך לפחות בשפות עברית, אנגלית		

פתרון לניהול מערכת ה-IVR של חברת AVAYA שכולל בין היתר את היכולות הבאות :

תיאור הדרישה	קיים (כן/לא)	פירוט נוסף/אפשרות פיתוח
אינטגרציה והתאימות של הפתרון למערכת Avaya Experience Portal		
המערכת תאפשר פיתוח תסריטי IVR באופן עצמאי ללא תלות בספק. יישום תסריטי IVR חדשים על גבי מערכת AVAYA ללא צורך במפתח		

		וישום בסביבת פיתוח של המערכת ה-IVR
		התממשקות של המערכת למערכות צד שלישי
		יכולת לבצע שינויים והגדרות בניתובי השיחות במערכת ה-IVR באמצעות כלי תפעולי נוח וקל לשימוש. המציע יפרט את היכולות בממשק הניהול ניתן לבצע שינויים בתסריטים, בצורה דינאמית ובזמן אמת בהתאם לצרכים המשתנים ללא צורך במפתח וביצוע שינויים בסביבת פיתוח של המערכת ה-IVR – Orchestration designer
		המערכת תאפשר לנהל רמות הרשאה שניתן למנהלי המערכת

ממשקי ניהול מתקדמים לניהול עצמאי של המערכות שכולל בין היתר את היכולות הבאות:

תיאור הדרישה	קיים (כן/לא)	פירוט נוסף/אפשרות פיתוח
ניהול הודעות קוליות/ הקלטות אולפן, ניהול שעות פעילות ותפריטים דינאמיים, ניהול נוסח הודעות SMS, בדגש על יכולות פתיחה/ סגירה/ הקמה מהירה של מוקדי שירות, עלי ידי צוות האחמשים במוקד באופן עצמאי ודינמי.		
ניהול העצמאי של הודעות / הקלטות / תפריטים לרבות העלאת הודעת, השמעת הודעה, הסרת הודעה, וכו' על ידי צוות האחמשים במוקד באופן עצמאי ודינמי. יש לפרט האם קיים כלי גמיש ונוח לניהול הקלטות (הקלטה, ועריכה).		
ניהול בצורה קלה ונוחה הודעות דינאמיות בדגש על המערכת תמיכה בהודעות והשמעתן בצורה דינאמית בהתאם לפרמטרים עסקיים / מידע/ מאפייני לקוחות הקופה.		
המערכת תאפשר רמת הרשאות למנהלי המערכת: לכל מוקד, קבוצה, ניתוב שיחה וברמה מערכתית.		
ניהול שעות פעילות במוקדים יכולת הגדרת שעות פעילות במוקדים השונים באמצעות כלי תפעולי, תוך תמיכה בשעות פעילויות שונות וכולל האפשרות לביצוע שינויים בזמן אמת.		

CALL BACK וחייגן – המערכות שכולל בין היתר את היכולות הבאות:

תיאור הדרישה	קיים (כן/לא)	פירוט נוסף/אפשרות פיתוח
אינטגרציה ותאימות של הפתרון למערכת Avaya Experience Portal יישום פתרון מתקדם לפתרון		

		Call Back וחייגן כאפליקציה על גבי תשתית מערכת ה- IVR של AVAYA.
		תמיכה בממשק הניהול התומך באופן מלא בעברית.
		תמיכה של הפתרון בניהול פעילות שיחות יוצאות/Dialer
		אינטגרציה למערכות CRM לצורכי הזדהות לקוח, רישום ועדכון שיחות במערכת ה- CRM - לדוגמא: שיחות חזרה ללקוח - Call Back וכו'.
		יכולת התאמה ספציפית ללקוח ולהגדרות שונות, עמידה בהנחיות ודרישות הרגולציה הישראלית בנושא שיחה חוזרת לצורך עמידה במענה וחזרה ללקוחות המתקשרים למוקדי השירות.
		במהלך המתנה של שיחה נכנסת תינתן האפשרות ללקוח להשאיר מספר טלפון לשיחה חוזרה - Call Back (באמצעות הקשות DTMF) כולל תמיכה בזיהוי אוטומטי של מספר הלקוח, בכדי שנציג יחזור אליו. בנוסף הלקוח יוכל גם לבחור את סוג השירות הרצוי / מועד מועדף לחזרה.
		הזנת מספר הטלפון אוטומטית לרשומות ה- Call Back של התור המתאים ו/או נושא השיחה ויופנה לנציגים עם המיומנות המתאימה. במידה והמתקשר או התור מוגדר VIP השיחה תנותב לראש תור ה- Call Back.
		במידה ולקוח אשר נרשם לשירות Call Back התקשר שוב למוקד ישמע הודעה ייעודית.
		המערכת תאפשר ייזום שיחות יוצאות (Outbound Calls) באופן אוטומטי ובאמצעות מנהל קמפיינים (ראה להלן).
		התממשקות ה-Dailer של הפתרון המוצע, לרבות, תמיכת הפתרון באופן העבודה במוקדי השימור של הקופה.
		הפתרון יכולל תמיכה בטעינת קמפיינים לשיחות יוצאות בצורה אוטומטית.
		במקרה של חיוג למספר תפוס או תא קולי או פקס או כל תוצאה אחרת ממענה של הלקוח ובהתאם תפעיל המערכת כללים עסקים בהתאם.
		יכולת טעינת לידים למערכת ממקורות שונים והפנייתם לנציג המתאים ביותר על בסיס קריטריונים מובנים כדוגמת: קמפיין יזום של הקופה, שיחות שננטשו, רשומות מצור קשר, מערכת לידים ספקים צד שלישי.

		המערכת תאפשר ייזום שיחות יוצאות (Outbound Calls) מבוקרות, תוך קליטת רשומות לחיוג מתוך מערכות מכבי באמצעות ממשק אוטומטי ו/או באמצעות טעינת קבצים.
--	--	--

דוחות זמן אמת והיסטוריים - דוחות זמן אמת לניהול של פעילות המוקדים הכוללים בין היתר את היכולות הבאות:

תיאור הדרישה	קיים (כן/לא)	פירוט נוסף/אפשרות פיתוח
תמיכה במסכי זמן אמת מפורטים לדרישות מנהלי המוקדים, תמיכה מלאה בעברית ואנגלית.		
קבלת חווי האם הנציג עובד מהמוקד או מהבית		
שליחת הודעות כתובות לנציגים בזמן אמת וקבלת הודעות מהנציגים בזמן אמת.		
יכולת העברה וניהול סקילים של הנציגים באמצעות מערכת הדוחות, הוצאה והכנסה של נציגים לסטטוסים זמין/ לא זמין.		
המערכת תאפשר רמת הרשאות למנהלי המערכת: לכל מוקד, קבוצה, ניתוב שיחה וברמה מערכתית.		
תמיכה בתכונות הבאות: כל מנהל מוקד / אחמ"ש יכול לבנות לעצמו את המסך ולקבל את הנתונים הרלוונטיים לו באופן עצמאי, ניתן לבנות הירארכיות מתקדמות במוקדים, מחלקות, צוותים, ניתן להגדיר הרשאות צפייה ומידור וכו'.		
התמיכה בהגדרות השונות לרבות: סוג הסטאטוסים, רמת הספים, הצבעים וכדומה, יוגדרו לפחות ברמת קבוצה, מוקד ומערכת ויבוצעו בכלי ניהול מרכזי המופעל ע"י אדמיניסטרטור המערכת ו/או האחמ"ש.		
תמיכה בהאזנה לנציג דרך מערכת ה- RT.		
הגדרת ספים ותצוגות בהתאם לפרמטרים הבאים: שיחות נכנסות ויוצאות (זמן שיחה) שיחות נענות ושיחות ננטשות במשמרת או בזמנית. המציע המשיב יפרט האם ניתן יהיה להגדיר ספים לכל אחד מנתונים אלו כך שלנציג תינתן התראה על מעבר הספים ע"י שינוי צבע, הבהוב וכו'.		
המציע יספק צילומי מסך של הדוחות של דוחות ה- RT ברמת, אחמ"ש, מנהל מערך מוקדים, פלאזמות וכו'.		

		תמיכה ביכולת של אחמ"ש להפעיל מסכי זמן אמת וניהול רלוונטיים על ידי לחיצה על שדה של דוח זמן אמת. למשל, על ידי לחיצה על שם נציג יופיע מסך לניהול המיומנויות שלו, על ידי לחיצה על שם Skill דוח זמן אמת של המוקד יופיע דוח פרטני של Skill.
		התמשקות למערכות BI ו- DB (במכבי קיימים) המאפשרות גישה לבסיסי נתונים בכלים סטנדרטים. לרבות, המערכת תאפשר לייצוא נתונים גולמיים לבסיסי נתונים ארגוניים של מכבי

דרישות נוספות :

תיאור הדרישה	קיים (כן/לא)	פירוט נוסף/אפשרות פיתוח
תמיכה מלאה בשפה העברית ניהול המערכת, ממשק נציג, דוחות כלי ניהול וכו' באופן מלא.		
ניהול הרשאות מידור של מנהלי המערכת ומנהלי המוקדים.		
יכולת מנהלי המערכת לבצע שינויים באופן עצמאי		
יכולת גיבוי ושחזור של המערכת		
התקנה על VMWare ויכולת דילוג מאתר לאתר ב- vMotion		
יכולת תפעול המערכת הן מאתר ה- DC הראשי של מכבי והן מאתר ה- DC המשי (DC), בעת נפילת האתר הראשי או בעת נפילת המרכזיה המופעלת מהאתר הראשי		
זמן משוער שנדרש לאספקת המערכת ותחילת עבודה. הגדרת אומדן לכמות שעות פיתוח נדרשות.		

3.4. מחיר המוצר/שירות :

מוצר	הערכת מחיר	מטבע מחיר
עלות רכישת המערכת, כולל תמיכה בכ-900 משתמשים בו זמנית		
עלות חד פעמית לאפיון, התאמות ויישום, הטמעה, התקנה, הדרכה וליווי		
עלות שנתית למערכת לרבות תמיכה, שדרוג גרסאות, תיקון באגים ורישיון		

יש לפרט בהצעת המחיר את הערכת המחיר לפרטים הבאים:

- מערכת כולל כל הרכיבים הנדרשים להפעלת התקינה
- עלויות תוכנה
- עלויות רישוי

3.5. מסמכים שיש לצרף להצעה

- 3.5.1. טופס מענה טכני לפי הנדרש מעלה
- 3.5.2. מפרט מלא של המוצע
- 3.5.3. תקני איכות
- 3.5.4. התייחסות לנספח אבטחת מידע (מקובל או שמבוקש שינוי)
- 3.5.5. פרוספקטים, אישורים, באם נדרש, או כל מידע רלבנטי אחר

3.6. הערות:

- 3.6.1. האומדן הינו הערכה בלבד.
- 3.6.2. המחירים אינם כוללים מע"מ.
- 3.6.3. אין להציע מחיר עם יותר מ-2 ספרות אחרי הנקודה.
- 3.6.4. ניתן להציע הצעות בש"ח/\$ ארה"ב/אירו/ין/ פרנק שוויצרי/ליש"ט/דולר קנדי/דולר אוסטרלי, למעט קריאת שרות אשר תתומחר בש"ח. לכל מטבע אחר יש לבקש אישור מראש.
- 3.6.5. תוקף ההצעה 90 ימים.

נספח א' – דרישות אבטחת מידע

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. לספק יהיו נהלי אבטחת מידע מעודכנים וזמינים לעובדי הספק. מכבי רשאית לבקש מהספק בכל עת עותק מנהלים אלו.
 - 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/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.
- 1.2. אבטחת מידע לוגית 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:

1.2.1. הגדרות

- 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).

1.2.1. הגדרות

- 1.2.1.1. מידע חסוי - מידע עסקי/ מידע רפואי/ מידע על עובדי מכבי
- 1.2.2. 1.2.3. 1.2.4. 1.2.5. 1.2.6. 1.2.7.1. 1.2.7.2. 1.2.7.3. 1.2.7.4. 1.2.7.5. 1.2.7.6. 1.2.7.7. 1.2.7.8. 1.2.8.
- 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 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. התחנה תינעל אוטומטית לאחר 5 שגיאות רצופות בהקשת הסיסמא.
 - 1.2.7.6. בכל תחנה יותקן נועל מסך עם סיסמא שיופעל לאחר 20 דקות לכל היותר.
 - 1.2.7.7. תותקן תכנת הגנה תקנית ומעודכנת כנגד וירוסים.
 - 1.2.7.8. מערכת ההפעלה המותקנת על התחנה מעודכנת בעדכוני האבטחה האחרונים שהופצו על ידי היצרן.
- 1.2.8. 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.

- 1.2.9. מדיה מגנטית או אופטית כנ"ל תאוחסן בתאום 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 סגור 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 WPA 2.
- 1.2.15. גישה מרוחקת למערכת הספק תבוצע לכל הפחות על בסיס הגדרות האבטחה הבאות:
 - 1.2.15.1. יבוצע "זיהוי חזק" כפול בעת הגישה לשירות.
 - 1.2.15.2. יוגדר לוג אירועים על השימוש בשירות.
 - 1.2.15.3. הגישה לשירות תבוצע על ידי שימוש בהצפנה על בסיס הסטנדרטים המקובלים בשוק.
- 1.3. אבטחת מסמכים
 - 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 בארונות, 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 המידע והגנת הסייבר במכבי בגין כל חשש לפגיעה, אובדן ו/או חשיפה של מסמכים המכילים מידע של מכבי.
- 1.4. גישה לרשת ולמערכות מכבי במקרה ובמהלך מתן השירותים למכבי יוקצה למי מטעם הספק שם משתמש לרשת ולמערכות מכבי הספק אחראי לכך שמשמש זה יפעל כאמור בסעיפים שלהלן, מכל אתר ומכל מחשב ממנו יתחבר לרשת מכבי:
- 1.4.1. לעובד הספק יוגדרו במסגרת תפקידו במכבי משתמש וסיסמא שימשו 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 שאינו מאובטח. במידת הצורך יש לבצע שימוש במקום אחסון מאובטח - אחסון בכספת פיזית לנייר ושימוש בהצפנה לקובץ מחשב.
- 1.4.3. הפעולות המבוצעות בעמדת עבודה המחוברת למערכת מכבי מנוטרות באמצעות מערכות הניטור והבקרה במכבי.
- 1.4.4. על עובד הספק הנעדר מעמדת העבודה להקפיד לנעול אותה באמצעות שומר מסך מוגן סיסמא.
- 1.4.5. 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.
- 1.4.6. אין לבצע כל שינוי בעמדת העבודה באורח עצמאי על ידי העובד, כולל התקנת תוכנות.
- 1.4.7. אין לשמור קבצים באופן מקומי על עמדת העבודה. הקבצים יישמרו על כונני הרשת הפנימית במקומות ייעודיים ע"פ רמת הסיווג שלהם.
- 1.4.8. 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:

07/07/2024

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. דרישות חיבור שרת לרשת מכבי.
 - 1.6.1. ההזדהות לשרת תנוהל ע"י מנגנון הזדהות מרכזי (MS Active Directory)
 - 1.6.2. השרת יתמוך בעדכוני א"מ נכון למדיניות מכבי (אחת לרבעון)
- 1.7. דרישות חיבור וניטור מערכת חדשה למרכז הסייבר
 - 1.7.1. כללי
 - 1.7.1.1. יוגדר ויופעל לוג אירועים מלא על כלל האירועים בכלל מרכיבי המערכת לרבות תשתית.
 - 1.7.1.2. תבוצע אינטגרציה להעברת לוג האירועים למערכת ה SIEM של מכבי (QRADAR); אינטגרציה זו תבוצע ע"י מכבי ובסיוע מלא של הספק.
 - 1.7.1.3. לוג האירועים ייושם על המרכיבים הבאים לכל הפחות:
 - 1.7.1.4. כל מודול ומערכת המאחסנת מידע של מכבי.
 - 1.7.1.5. כל רכיב בשרת: מערכת הפעלה, מסד הנתונים, וה-GUI.
 - 1.7.1.6. כל רכיב במערכת: אתר משתמשים, backoffice וכו'.
 - 1.7.2. ירשם לוג אירועים אודות הבאים לכל הפחות
 - 1.7.2.1. הזדהות בכניסה למערכת, לרבות ניסיונות הזדהות כושלים;
 - 1.7.2.2. כל סוג גישה לנתונים, לרבות קריאה בלבד;
 - 1.7.2.3. כל גישה ללוג האירועים, שינוי הגדרות בו או מחיקתו;
 - 1.7.2.4. כל פעולה המבוצעת על ידי משתמשי ניהול מערכת \ שרת;
 - 1.7.2.5. שינוי הגדרות מערכת. לרבות שינוי במנגנון המשתמשים וההרשאות;
 - 1.7.2.6. כל סוג אירוע נוסף ככל שיקבע לפי רלוונטיות ע"י מנהל הגנת הסייבר במכבי.
 - 1.7.3. לוג האירועים, יכיל, לכל הפחות, את הנתונים הבאים אודות הפעולה
 - 1.7.3.1. מועד ביצוע הפעולה;
 - 1.7.3.2. שם משתמש שביצע את הפעולה ועל מי או על מה בוצעה הפעולה;
 - 1.7.3.3. כתובת מקור
 - 1.7.3.4. סוג רכיב המקור (דוג' דפדפן / PC / טלפון וכיו"ב);
 - 1.7.3.5. כתובת יעד;
 - 1.7.3.6. שם הפעולה;
 - 1.7.3.7. תיאור הפעולה;
 - 1.7.3.8. סטטוס – הצלחה/כישלון.
 - 1.7.4. סוגי התממשקות למערכת ה- SIEM לפי תעודף
 - 1.7.4.1. Syslog
 - 1.7.4.1.1. One Line
 - 1.7.4.2. גישה למסד הנתונים (DB)
 - 1.7.4.2.1. על המערכת להכיל Table\View ייעודיים המכילים את כלל האירועים (Events).
 - 1.7.4.2.2. על הספק להעביר את הנתונים הנדרשים לאינטגרציה לרבות שם משתמש בעל הרשאות קריאה לגישה לDB, כתובת, שם Table\View וכיו"ב.
 - 1.7.4.2.3. יש לוודא כי עמודת המפתח ב- Table\View הינה מסוג \ Timestamp unique ID
 - 1.7.4.3. Rest API
 - 1.7.4.3.1. הממשק נדרש להיות מוחצן ע"י השרת/מערכת.

- File Reader .1.7.4.4
 - גישה לשרת קבצים\שרת אחסון (445\ 22 סטנדרטי כברירת מחדל) או .1.7.4.4.1
 - פרוטוקוליי file share אחרים.
 - .CLEAR TEXT .1.7.4.4.2
 - מבנה הלוג הנדרש .1.7.5
 - SYSLOG .1.7.5.1
 - RFC3164 ·
 - RFC5424 ·
 - JSON ·
 - CEF ·
 - LEEF ·
 - File Reader .1.7.5.2
 - CSV (יש לוודא שכל שדה יהיה מופרד עם key value)