

13/07/2026

בקשה לקבלת מידע (RFI)

שירות מלא מקצה לקצה לקיבוע אורתופדי באמצעות גבס תלת-ממד מותאם אישית לחברי מכבי כחלופה לגבס רגיל במקרים קליניים מתאימים (להלן - "הבקשה")

1. כללי

- 1.1 מכבי שירותי בריאות (להלן - "מכבי") מעוניינת לקבל מידע מספקים המסוגלים להפעיל שירות מלא מקצה לקצה לקיבוע אורתופדי באמצעות גבס תלת-ממד מותאם אישית, כחלופה לגבס רגיל (לבן) או גבס קל במקרים קליניים מתאימים.
- 1.2 את המענה יש למלא על גבי מסמך זה או על גבי מסמך של המציע ולשלוח אל מר. שחר מסר לדואר אלקטרוני: **messer_s@mac.org.il עד לתאריך 11/08/2026**.
- 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 המשיבים 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 וענייניים.
- 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 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. מטרת הבקשה

מכבי מבקשת למפות ספקים המסוגלים להפעיל בישראל שירות מלא ומנוהל בתחום גבס תלת-ממד מותאם אישית, במודל שבו הספק אחראי לכלל התהליך, החל מאספקת ציוד הסריקה והכשרת הצוותים ועד לייצור, גבייה פרטית, אספקה ושירות לאחר המכירה.

יובהר כי מכבי אינה מבקשת לרכוש או להפעיל מדפסות תלת-ממד, והייצור יבוצע באחריות הספק או מי מטעמו.

- זיהוי ספקים המסוגלים לספק שירות מלא מקצה לקצה במסגרת רפואת הקהילה.
- הבנת התוויות השימוש, האזורים האנטומיים, המגבלות והאישורים הרגולטוריים של המוצר.
- הבנת מודל ההפעלה: סריקה, ייצור, אספקה, שירות, סליקה, ציוד, חיבוריות ועלויות.
- בחינת מערך השירות והתמיכה, לרבות מוקד שירות לקוחות, טיפול בהחלפות, זיכויים, תקלות, מתן מידע ללקוחות, דוחות ועמידה ברמות שירות.
- בחינת הערך השירותי למטופל, לרבות נוחות, משקל, אוורור, עמידות למים, אסתטיקה, צבעים / דוגמאות והוראות שימוש.

3. מידע כללי על החברה והפתרון

פירוט מבוקש	נושא
שם החברה, שנת הקמה, תחומי התמחות, מספר עובדים, אתר אינטרנט, איש קשר ופרטי התקשרות.	פרטי החברה
ניסיון בהפעלת שירות מלא בתחום גבס תלת-ממד, ותק הטכנולוגיה בארץ ובעולם, מספר גבסים שיוצרו, אתרים פעילים ולקוחות מרכזיים.	ניסיון ופעילות
שם היצרן או הגורם המבצע את הייצור, מיקום הייצור, שנות ניסיון, תקני איכות והסכמים עם ספקי משנה, ככל שקיימים.	יצרן / מערך ייצור

פירוט מבוקש	נושא
אופן אספקת ציוד הסריקה והכשרת הצוותים, פתיחת הזמנה וסליקה פרטית, ייצור, בקרת איכות, משלוח, שירות לקוחות וטיפול בהחלפות או זיכויים.	מודל שירות

4. המענה המבוקש - טבלת מענה מרכזית

על המשיב להתייחס לכל נושא בטבלה: כן / לא / חלקי + פירוט תמציתי. מטרת הטבלה היא מענה ראשוני קצר ובר-השוואה, ללא כניסה לאפיון מפורט בשלב זה.

פירוט נדרש	התייחסות המשיב	נושא / דרישה
ייעוד המוצר כחלופה לגבס רגיל/לבן או גבס קל; אישור רגולטורי; אזורים אנטומיים; סוגי שברים; מגבלות; התאמה לילדים / מבוגרים.	כן / לא / חלקי	מוצר, רגולציה והתוויות שימוש
אחריות הספק לכלל רכיבי השירות: ציוד סריקה, הדרכה, מערכת הזמנות, סליקה פרטית, ייצור, בקרת איכות, משלוח, שירות ותמיכה.	כן / לא / חלקי	מודל שירות מלא מקצה לקצה
אספקת ציוד הסריקה על ידי הספק; אופן הפריסה במרפאות ובמוקדים; תחזוקה והחלפה; מי רשאי לבצע סריקה; משך ותכולת ההכשרה.	כן / לא / חלקי	ציוד סריקה והכשרה
פתיחת הזמנה והעלאת סריקה; גבייה דיגיטלית ישירות מחבר מכבי מול הספק, ללא התערבות מכבי; קבלה / חשבונית, ביטול והחזרים.	כן / לא / חלקי	מערכת הזמנות וסליקה פרטית

פירוט נדרש	התייחסות המשיב	נושא / דרישה
הייצור מתבצע על ידי הספק או צד שלישי מטעמו. מכבי אינה רוכשת או מפעילה מדפסות. יש לפרט מיקום ייצור, ספקי משנה ותהליך הייצור.	כן / לא / חלקי	ייצור באחריות הספק
בקרת איכות על הסריקה ועל הגבס; זמני ייצור; משלוח לבית המטופל או למרפאה; מעקב ועדכון המטופל.	כן / לא / חלקי	בקרת איכות ואספקה
מוקד שירות לקוחות זמין בישראל; שעות פעילות; ערוצי קשר; מתן מידע ללקוחות; תמיכה טכנית ותפעולית.	כן / לא / חלקי	שירות לקוחות ותמיכה
טיפול בפגם, אי התאמה, טעות מידה או שבר במוצר; ייצור חוזר; החלפה; ביטול וזיכוי; זמני טיפול ואחריות.	כן / לא / חלקי	החלפות, זיכויים וייצור חוזר
נוחות, משקל, אוורור, עמידות למים, צבעים, דוגמאות, עיצובים, אפשרות להטבעת לוגו מכבי והוראות שימוש.	כן / לא / חלקי	חווית מטופל והתאמה אישית
ציוד הסריקה יתמוך בחיבור באמצעות WIFI, SIM/eSIM או נטסטיק ויאפשר עבודה ללא תלות הכרחית ברשת מכבי.	כן / לא / חלקי	ציוד קצה וחיבוריות
דוחות רכישות לפי מרפאה / מוקד / רופא; זמני ייצור ואספקה; החלפות, ביטולים, זיכויים	כן / לא / חלקי	דוחות, SLA וניהול מידע

נושא / דרישה	התייחסות המשיב	פירוט נדרש
		וויצור חוזר; עמידה ב-SLA; שמירת מידע והרשאות.
הפעלה עצמאית ואינטגרציה עתידית	כן / לא / חלקי	הפעלת השירות ללא אינטגרציה למערכות מכבי בשלב הראשון; יכולת התממשקות עתידית, ככל שתידרש, לרבות שמירת קובצי הסריקה בתיק המטופל.

5. מודל עסקי ותמחור ראשוני

המשיב מתבקש לפרט בקצרה את המודל העסקי והתמחורי המוצע להפעלת שירות מלא מקצה לקצה, לרבות מחיר לגבס, מה כלול במחיר, אופן אספקת ציוד הסריקה, עלויות נוספות ככל שקיימות, אופן הגבייה הישירה מהחבר ותנאים מסחריים נוספים.

תיאור הפריט	הערכת עלות יחיד כולל מע"מ	הערכת עלות כוללת כולל מע"מ	מטבע	הערות
אומדן עלויות				
מחיר לגבס תלת-ממדי / בודד, לפי אזור אנטומי גיל / גודל / סוג מוצר, ככל שקיימת הבחנה				
ציוד סריקה				
חיבור תקשורת- אינטרנט ללא תלות ב- WIFI מכבי				
רישיון מערכת				
הדרכות				
תמיכה טכנית				

				משלוח לבית הלקוח/ מוקד רפואי/מרפאה
				תחזוקה שנתית
				אחר

סעיף 6 - לקוחות ממליצים

המשיב מתבקש להציג, ככל שניתן, לקוחות קיימים בארץ או בעולם, בדגש על ארגוני בריאות, מרפאות אורתופדיות, בתי חולים או רפואת קהילה.

לקוח	תחום	תיאור שימוש	איש קשר	טלפון

7. מסמכים לצירוף והמשך תהליך

המשיב מתבקש לצרף, ככל שקיים ורלוונטי: דפי מוצר, מסמכי אישור רגולטורי / הצהרת יצרן / Intended Use, תיאור תהליך הפעלה, מפרט מוצר קצר, חומרי הסברה למטופל, תמחור ראשוני, דוגמאות לדוחות פעילות והמלצות לקוחות.

מכבי רשאית לבקש הבהרות, הדגמה או מסמכים נוספים. ככל שהפתרון יימצא רלוונטי להמשך בחינה, יידרש הספק להתייחס גם לנספחי הטכנולוגיה ואבטחת המידע המצורפים למסמך.

נספח א': דרישות שירות, תפעול וטכנולוגיה

על הספק להתייחס לכל אחת מהדרישות בטבלה להלן. מטרת הנספח היא לבחון שירות מלא ומנוהל שבו הספק מספק את ציוד הסריקה, מפעיל את מערכת ההזמנות והסליקה, אחראי לייצור בעצמו או באמצעות ספק משנה, מספק את הגבס ומעניק שירות ותמיכה לאחר המכירה. מכבי אינה רוכשת או מפעילה מדפסות תלת-ממד.

נושא / דרישה	התייחסות המשיב	פירוט הספק
מערכת דיגיטלית לפתיחת הזמנה, העלאת סריקה וניהול סטטוס	כן / לא / חלקי	יש לפרט שם מערכת, אופן גישה, משתמשים מורשים, תהליך פתיחת הזמנה, העלאת סריקה ומעקב עד למסירה.
שמירת נתוני חברים ושיוך ההזמנה	כן / לא / חלקי	יש לפרט אילו נתונים נשמרים וכיצד משויכת ההזמנה לחבר, מרפאה / מוקד, רופא, איש צוות, אזור אנטומי וסטטוס התהליך.
אספקת ציוד סריקה וניהולו	כן / לא / חלקי	הספק יספק את כל ציוד הסריקה הנדרש. יש לפרט סוגי ציוד, מודל אספקה, פריסה, תחזוקה, תיקון, החלפה, אובדן ואחריות.
חיבוריות ותקשורת לציוד הסריקה	כן / לא / חלקי	יש לפרט תמיכה ב-WIFI, SIM/eSIM ונטסטיק, וכן אפשרות עבודה ללא תלות ברשת מכבי בכל שלבי הסריקה, ההזמנה והתשלום.
הכשרה וניהול משתמשים	כן / לא / חלקי	יש לפרט מי רשאי לבצע סריקה והזמנה, תכולת ההכשרה, משך ההכשרה, ריענונים, פתיחת משתמשים והרשאות לפי אתר ותפקיד.
גבייה (דיגיטלית/ טלפונית) פרטית ישירות מול הספק	כן / לא / חלקי	יש לפרט אמצעי תשלום, מסלוקה, מועד חיוב, הנפקת קבלה / חשבונית, ביטול, החזרים וזיכויים. מכבי אינה צד בתהליך הגבייה.
ייצור באחריות הספק או ספק משנה	כן / לא / חלקי	יש לפרט היכן מתבצע הייצור, מי הגורם המבצע, תקני איכות ספקי משנה ובקורות. מובהר כי מכבי אינה רוכשת או מפעילה מדפסות.
בקרת איכות וניהול מחזור ההזמנה	כן / לא / חלקי	יש לפרט בקרת איכות על הסריקה והמוצר, סטטוסים אפשריים, טיפול בסריקה לא תקינה, עיכובים, ביטול וייצור חוזר.
משלוח ועדכון המטופל	כן / לא / חלקי	יש לפרט זמני ייצור ומשלוח, אפשרויות אספקה לבית המטופל או למרפאה, אופן המעקב והודעות מסרון / דוא"ל לאורך התהליך.
מוקד שירות לקוחות ותמיכה	כן / לא / חלקי	יש לפרט שעות פעילות, שפות, ערוצי שירות, זמני תגובה, מתן מידע ללקוחות ותמיכה בציוד הסריקה ובמערכת ההזמנות.
החלפות, זיכויים, החזרים וייצור חוזר	כן / לא / חלקי	יש לפרט תהליך טיפול באי התאמה, פגם, טעות מידה או שבר במוצר, לרבות אחריות, החלפה, ייצור חוזר, זיכוי והחזר כספי.
דוחות ניהוליים ומעקב אחר SLA	כן / לא / חלקי	יש לפרט דוחות לפי מרפאה / מוקד / רופא / איש צוות, מספר רכישות, ביטולים, החלפות, ייצור חוזר, תקלות, זמני ייצור ואספקה ועמידה ב-SLA
ניהול מחזור חיי המידע ואבטחתו	כן / לא / חלקי	יש לפרט סוגי מידע הנשמרים, מיקום השמירה, הרשאות, משך שמירה, מחיקה / אנונימיזציה, הצפנה, ספקי ענן וספקי משנה.

הפעלה עצמאית ואינטגרציה עתידית	כן / לא / חלקי	יש לפרט יכולת הפעלה ללא אינטגרציה למערכות מכבי וכן אפשרות התממשקות עתידית, ככל שתידרש, לרבות שמירת קובצי סריקה בתיק המטופל וייצוא נתונים למכבי.
--------------------------------	----------------	---

נספח ב' : אבטחת מידע

על הספק המציע לעמוד בדרישות מצ"ב

1.1 כללי

- 11.1.1 אצל הספק יוגדר איש קשר אחראי לאבטחת המידע שבאחריותו לוודא את יישומן של הדרישות שיובאו להלן.
- 11.1.2 לספק יהיו נהלי אבטחת מידע מעודכנים וזמינים לעובדי הספק. מכבי רשאית לבקש מהספק בכל עת עותק מנהלים אלו.
- 11.1.3 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.
- 11.1.4 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.
- 11.1.5 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.
- 11.1.6 כל מידע המגיע לידי הספק ומי מטעמו יישמר ולא יעשה בו שימוש שלא לצורך הפעילות מול מכבי.
- 11.1.7 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.
- 11.1.8 הספק מתחייב כי כל ספקי המשנה שלו עומדים בכל דרישות אבטחת המידע במסמך זה.
- 11.1.9 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.
- 11.1.10 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.

- 11.1.11 הספק מתחייב לאפשר לנציג מכבי לערוך ביקורת אבטחה בכל עת. הביקורת תבוצע בתאום עם הספק.
- 11.1.12 הספק אחראי להתאים את רמת אבטחת המידע שלו לסטנדרטים המקובלים בשוק.
- 11.2 דרישות אבטחת מידע למכשיר רפואי
- 11.2.1 הספק יעביר למחלקת אבטחת מידע והגנת הסייבר במכבי מסמך MDS2 מלא עבור המכשור הרפואי.
- 11.2.2 על פי המענה במסמך ה-MDS2 יינתנו דרישות אבטחת מידע למכשיר הרפואי במסגרת הטמעתו במכבי.
- 11.2.3 כחלק משלב ההטמעה, מכבי תהא רשאית לבצע מבדק סיכוני אבטחת מידע כולל (אך לא מוגבל ל) בחינת סיכוני אבטחת מידע ביישום, ברשת, ומבדק חדירה ממשקים פנימיים וחיצוניים. הספק מתחייב לטפל בסיכוני האבטחה המטרפדים עמידת מכבי בדרישות חוק, תקן ורגולציה.
- 11.2.4 על הספק לשמור על רמת אבטחת המידע של כלל המערכות והטכנולוגיות הנרכשות או המפותחות, כולל תת המרכיבים שלהן לאורך כל תקופת ההסכם:
- 11.2.4.1 על הספק לוודא כי המערכת מותקנת ומוקשחת על פי הנחיות היצרן.
- 11.2.4.2 הספק מתחייב כי נקט באמצעים הדרושים על מנת להבטיח שהמכשיר והתוכנה בעת התקנתם במכבי יהיו נקיים מקוד זדוני.
- 11.2.4.3 על הספק לבצע שדרוגים ועדכוני אבטחת מידע לפתרון תקלות ולצרכי אבטחת המערכת, על מנת לתקן כל נקודת תורפה שפורסמה על ידי היצרן.
- 11.2.4.4 כאשר עדכוני האבטחה כרוכים בהתקנת עדכוני צד שלישי, הספק יספק הודעה בכתב למכבי כי התיקון אומת ככזה שאינו משפיע על הפעילות השוטפת של המערכות.
- 11.2.5 במקרה וקיים במערכת שימוש בטכנולוגיה של Bluetooth, על הספק לפעול על פי ההגדרות הבאות:
- 11.2.5.1 המכשיר יעבוד ברמת Security Level 3/ Security Level 4 לפחות:
- 11.2.5.1.1 Level 4: Authenticated link key using Secure Connections required
- 11.2.5.1.2 Level 3: Authenticated link key required
- 11.2.5.2 מכשיר בעל קישוריות אלחוטית, יתקשר רק באמצעות פרוטוקול Bluetooth גרסה 5.
- 11.2.5.3 צימוד בין המכשיר לבין התקן נוסף (דוגמת טלפון חכם), יתבצע רק על ידי הקשת סיסמא.
- 11.2.5.4 רק המכשיר יהיה בעל היכולת ליזום צימוד Bluetooth.
- 11.2.5.5 יצירת צימוד Bluetooth תחייב פעולה אקטיבית על המכשיר (לדוגמא לחיצה על כפתור ייעודי במכשיר לצורך צימוד).
- 11.2.5.6 המכשיר לא יאפשר צימוד של יותר ממכשיר אחד בו זמנית.
- 11.2.5.7 פרוטוקולי ההצפנה המאושרים בעת הצפנת תקשורת BLUETOOTH הינם AES-CMAC ו-P-256 elliptic curve
- 11.2.6 במקרה וקיים במערכת שימוש בטכנולוגיה של רשת אלחוטית (WIFI), הרשת תאובטח לכל הפחות ע"י שימוש בהגדרות הבאות:
- 11.2.6.1 הרשת (SSID) תוגדר במצב מוסתר שאינו גלוי לכל.

11.2.6.2 יבוצע שימוש בפרוטוקול WPA2.

11.2.7 הספק יודיע למכבי תוך 24 שעות מעת גילוי על חשיפות של פרצות אבטחת מידע העלולות לפגוע באבטחה של המערכת (פגיעה בסודיות, שלמות או זמינות המערכת). נושאים אלו יתקנו במהירות האפשרית.

11.2.8 מערכות רפואיות וציוד אחר הכוללים מדיה כגון כוננים קשיחים, אופטיים וכו', שעליהם נשמר מידע של מכבי ו/או מבטחיה, לא יוחזרו לספק בסיום ההסכם/ בעת החלפת המוצר באחר אלמלא מולאו אחד מהתנאים הבאים:

11.2.8.1 הספק יקבל את המערכת ללא התקן המדיה.

11.2.8.2 ניתן למחוק את המידע על ההתקן באופן שלא יהיה ניתן לשחזרו.

11.2.9 הגישה של המערכת למערכות מכבי תבצע על פי הנחיות אבטחת מידע שיינתנו במסגרת ההטמעה.

11.2.10 הגישה של המערכת למערכות מכבי תבצע באמצעות שם משתמש וסיסמה של מכבי ותחול עליו מדיניות הסיסמאות של מכבי שלהלן:

11.2.10.1 אורך הסיסמא יהיה לפחות שבעה תווים.

11.2.10.2 הסיסמאות יוחלפו כל שלושה חודשים לפחות.

11.2.10.3 התחנה תינעל אוטומטית לאחר 5 שגיאות רצופות בהקשת הסיסמא .

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

11.2.11 העברת המידע מהמערכת למערכות מכבי תבצע באופן מוצפן.

11.2.12 במקרה ויש חומרה שמתחברת לרשת מכבי (מכשיר רפואי/ מערכת וכדומה), על רכיב התקשורת לתמוך בפרוטוקול האימות 802.1X וכיוצא מכך לתמוך באלגוריתמי האימות: EAP-TLS, EAP-TTLS, EAP מוגן (PEAP) - I EAP Cisco Wireless Light Extensible Authentication Protocol (LEAP).

11.3 אחסון מידע

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

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

11.4 הצפנת המידע

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

11.4.1.2 ההצפנה תבוצע בהתאם לסטנדרטים המקובלים בשוק.

11.4.1.3 מפתחות ההצפנה יישמרו באופן בלעדי בידי הארגון במידת האפשר.

11.5 העברת מידע

11.5.1.1 העברת המידע תבוצע בתווך מזהה ומוצפן.

11.6 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:

11.6.1 הגדרות

- 11.6.1.1 מידע חסוי - מידע עסקי/ מידע רפואי/ מידע על עובדי מכבי
- 11.6.1.2 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 ואלומות במשפחה
- 11.6.2 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 בול"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).
- 11.6.3 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.
- 11.6.4 הספק יודא הצפנה של קבצים המכילים מידע של מכבי המסווג כ"חסוי או חסוי ביותר" ע"פ מדיניות סיווג המידע של מכבי.
- 11.6.5 קבצים המכילים מידע של מכבי המסווג כ"חסוי או חסוי ביותר" ע"פ מדיניות סיווג המידע של מכבי יועברו מהספק אל מכבי באופן מוצפן.
- 11.6.6 אין להעביר קבצים המכילים מידע של מכבי בדוא"ל ואו בכל אמצעי תקשורת אחר לגורמים אחרים ללא אישור בכתב ממכבי.
- 11.6.7 בתחנות העבודה של הספק תשמר אבטחת המידע באופן הבא:
- 11.6.7.1 לא יישמרו קבצי מכבי על הדיסק הקשיח של התחנה (למעט לגבי חברה או יחיד ללא רשת משתמשים).
- 11.6.7.2 הכניסה לתחנה תהיה באמצעות USER ID וסיסמא אישית
- 11.6.7.3 אורך הסיסמא יהיה לפחות שבעה תווים.
- 11.6.7.4 הסיסמאות יוחלפו כל שלושה חודשים לפחות.
- 11.6.7.5 משתמש שנכשל בעת ניסיון הזדהות 5 פעמים ברציפות ינעל באופן אוטומטי.
- 11.6.7.6 נדרשת אכיפה שנועלת את מחשבי הארגון לאחר 20 דקות ללא שימוש במחשב.
- 11.6.7.7 תותקן תכנת הגנה תקינית ומעודכנת כנגד וירוסים.
- 11.6.7.8 מערכת ההפעלה המותקנת על תחנות העבודה נדרשות להיות מעודכנת בעדכוני האבטחה האחרונים שהופצו על ידי היצרן.

- 11.6.8 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.
- 11.6.9 מדיה מגנטית או אופטית כנ"ל תאוחסן בתיאום עם מכבי במקום שהגישה אליו תתאפשר למורשי גישה בלבד.
- 11.6.10 גיבויים יבוצעו בצורה מסודרת וישמרו במקום סגור ונעול עם גישה לאחראי על הגיבויים בלבד. כמו כן על הספק לקיים נוהל שחזור תקופתי לגיבויים.
- 11.6.11 אין להעביר קלטות עם גיבויים של קבצים המכילים מידע של מכבי לגופים חיצוניים ללא ידוע מראש.
- 11.6.12 כל מדיה מגנטית או אופטית או דוח המהווים תוצרי עיבוד מנתוני מכבי יאוחסנו בארון נעול וכן יושמדו וייגרסו לאחר השימוש.
- 11.6.13 הספק מתחייב להודיע מידית למנהל אבטחת המידע והגנת הסייבר במכבי בגין כל חשש לפגיעה, אובדן ו/או חשיפה של קבצים המכילים מידע של מכבי.
- 11.6.14 במידה וקיים שימוש בטכנולוגיה של רשת אלחוטית (wifi), הרשת תאובטח לכל הפחות ע"י שימוש בהגדרות הבאות:
- 11.6.14.1 הרשת (ssid) תוגדר במצב מוסתר שאינו גלוי לכל.
 - 11.6.14.2 יבוצע שימוש בפרוטוקול האבטחה WPA 2.
- 11.6.15 גישה מרוחקת למערכת הספק תבוצע לכל הפחות על בסיס הגדרות האבטחה הבאות:
- 11.6.15.1 הגדרת הזדהות רב שלבית בעת הגישה לשירות (MFA).
 - 11.6.15.2 יוגדר לוג אירועים מלא על השימוש בשירות.
 - 11.6.15.3 הגישה לשירות והתעבורה יוצפנו על בסיס הסטנדרטים המקובלים בשוק.
- 11.7 אבטחת מסמכים
- 11.7.1 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.
- 11.7.2 מסמכים המכילים מידע של מכבי ישמרו נעולים בארונות, מגירה, ארון או כספת שהוקצו לצורך זה בלבד.
- 11.7.3 הגישה למסמכים אילו תותר רק למי שעבודתם ותפקידם אצל הספק מחייבים זאת, ולכאלו שחתמו על התחייבות לשמירת סודיות מול מכבי.
- 11.7.4 אין להעביר מסמכים המכילים חומר מודפס של מכבי לגורמים אחרים בכל אמצעי (פקס, דואר ישראל וכו'), ללא אישור כתוב ממכבי.
- 11.7.5 אין להשאיר מסמכים עם חומר של מכבי על השולחן/במדפסת בסוף יום העבודה.
- 11.7.6 יש לגרוס מסמכים המכילים מידע של מכבי בתום השימוש בהם.

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

11.8 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:

11.8.1 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.

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

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

11.8.4 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 .

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

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

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

11.9 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:

11.9.1 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.

11.9.2 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.

11.9.3 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.

11.9.4 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.

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

11.10 ארכיטקטורה

- 11.10.1 האתרים יהיו תחת Domain מכבי (כלומר URL של האתרים יהיו ב Domain מכבי).
- 11.10.2 חל איסור עקב מבטלות טכנולוגיות לעבוד עם שירותים המבוססים על פרוטוקול Web socket. במידת הצורך ניתן לפנות לאבטחת מידע והגנת הסייבר במכבי על מנת לאפיין פתרון חלופי.
- 11.10.3 שליחת ה- SMS/ WhatsApp תבוצע אך ורק למספרי הטלפון המעודכנים במכבי. זהות השולח תהיה מכבי שירותי בריאות.
- 11.10.4 שליחת המיילים יועברו מכתובת של מכבי בלבד. לצורך כך הספק מתחייב להעביר כתובות IP למכבי לצורך הגדרת SPF.
- 11.10.5 ממשק הניהול – יוגבל ברמת תקשורת לכניסה רק ממחשבי מכבי, ומחשבי הספק (לצורכי תמיכה).
- 11.10.6 הספק יישם את הגדרות האבטחה הבאות:
 - 11.10.6.1 האתרים המשמשים את הפתרון ימוגנו על ידי Web application firewall של מכבי שירותי בריאות.
 - 11.10.6.2 ממשק ניהול (מכל סוג) לא יהיה נגיש לכל כתובות האינטרנט, אלא יפתח ב FW רק לכתובות ספציפיות של מכבי ושל הספק.
 - 11.10.6.3 כל הנתונים ישמרו מחוץ לשרת ה WEB בשרת מסד הנתונים ייעודי באיזור ממודר ברשת.
 - 11.10.6.4 שרת מסד הנתונים ישב בסגמנט ייעודי מופרד ב FW מסגמנט שרת ה WEB. סיגמנט זה יהיה חסום לגישה אל ומ- האינטרנט.
 - 11.10.6.5 עובדי מכבי יזדהו למערכת ע"י הזדהות מול IDP של מכבי (מימוש יתבצע ע"י SAMEL).
 - 11.10.6.6 תבוצע הפרדה בין שרתי מכבי לשרתי הספק ושרתי לקוחות נוספים. ההפרדה תבוצע לבאים: שרת זהויות, מסדי נתונים, שרתי WEB ואפליקציה.
 - 11.10.6.7 תבוצע הפרדה בין סביבת הייצור לסביבת הפיתוח והבדיקות. ההפרדה תבוצע הן ברמת אפליקציה והן ברמת תשתיות (שרת ווב, שרת מסד נתונים וכו').
 - 11.10.6.8 יוגדרו סיגמנטים ייעודיים עבור שרתי מכבי אשר יופרדו מבחינת תקשורת משאר שרתי הספק (הכוונה למערכות ההפעלה, ולא לברזלים המחזיקים את כלל השרתים הווירטואליים).
 - 11.10.6.9 באתרים יופעלו שירותי מערכות הבקרה הבאים (השירותים למערכות יופעלו במוד הגנה אקטיבית (חסימה) ולא במוד למידה).
 - 11.10.6.9.1 FW – אפיון והגדרה של ה WAF באופן אקטיבי על בסיס התאמה לאתר האינטרנט.
 - 11.10.6.9.2 IPS
 - 11.10.6.9.3 ממשק הפלטפורמה ל- WAF של מכבי
 - 11.10.6.9.4 Anti DOS\DDOS (להגנה ספציפית על אתרי מכבי).

- 11.10.6.9.5 אנטי וירוס - האנטי וירוס יעודכן ברמה יומית.
- 11.10.6.9.6 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.
- 11.10.6.9.7 הקשחת שרתים - כל מערכות המידע יעברו הקשחה על פי הסטנדרטים המקובלים בשוק.
- 11.10.6.10 מועמדים חיצוניים (שאינם עובדי מכבי) יזדהו למערכת באמצעות חשבון אישי באתר.
- 11.10.6.11 גישה לשירותים מחוץ לרשת מכבי עבור עובדי מכבי תתאפשר רק מרשת מכבי.

11.11 ממשקי Web Service:

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

- 11.11.1 תצורת MTLS עם זיהוי תעודות דו כיווני (הכולל תעודה דיגיטלית ייעודית לשרת, ותעודה שניה ייעודית לצד ה-Client).
- 11.11.2 גישה לשירות (API) דורשת פניה באמצעות כתובת IP קבועה בלבד. לא תתאפשר פניה לשירות מכתובת DHCP או כתובת שאינה קבועה.
- 11.11.3 בכל הממשקים מול מכבי, מכבי תהווה את צד ה-Server בממשק, כאשר הספק הוא ה-Client.
- 11.11.4 כל גישה ממשק לשירות תבוצע דרך רכיב API MGMT (API F5, DP APIC, וכו') שיבצע הזדהות, מידור ו Schema validation.
- 11.11.5 לכל שירות יהיה הזדהות ייחודית והרשאות ייחודיות מול שירותים אחרים.
- 11.11.6
- 11.11.7 מכבי תוכל לספק תעודות דיגיטליות לכל הצדדים בתהליך התשתיתיים והאפליקטיביים, הכוללים את תשתיות הרשת (Active Directory לדוגמה), מסדי הנתונים, האפליקציה, וה- WEB.
- 11.11.8 במידת הצורך יועבר פירוט מלא של דרישות הגנה מפני התקפות אפליקטיביות.
- 11.12 הצפנה
- 11.12.1 דרישות תעודת הצפנה:
- 11.12.1.1 תעודת הספק תהיה מ issuer חיצוני ולא CA מקומי
- 11.12.1.2 אלגוריתם של התעודה תהיה sha256
- 11.12.1.3 התעודה תכיל CRL Distribution Points
- 11.12.2 דרישות לגבי ההצפנה:
- 11.12.2.1 העבודה מול הספק תהיה בתווך TLS ver. 1.2 or above
- 11.12.2.2 התקשורת והמידע יהיו חתומים למוצפנים ע"י התעודות. (כולל ה response מהספק)
- 11.13 ניטור אירועים
- 11.13.1 יוגדר ויופעל לוג אירועים מלא על כלל האירועים בכלל מרכיבי המערכת.

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

11.13.3 לוג האירועים יוגדר על הבאים:

11.13.3.1 בכל מודול ומערכת שמאחסנת מידע של מכבי.

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

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

11.13.4 לוג אירועים יופעל על האירועים הבאים:

11.13.4.1 כניסות למערכת – מוצלחות או כישלונות.

11.13.4.2 כל גישה לנתונים, כולל קריאה בלבד.

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

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

11.13.4.5 שינוי הגדרות מערכת. כולל שינוי במערכת המשתמשים וההרשאות.

11.13.5 רישום כל אירוע יכלול את הערכים הבאים:

11.13.5.1 מועד ביצוע הפעולה.

11.13.5.2 שם משתמש מבצע הפעולה.

11.13.5.3 כתובת מקור.

11.13.5.4 סוג ה-Client.

11.13.5.5 שם הפעולה.

11.13.5.6 סטטוס – הצלחה/כישלון.

11.13.5.7 תיאור הפעולה.

11.14 פיתוח מאובטח

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

11.14.1 האתר יפותח בסטנדרט פיתוח מאובטח – OWASP-Top 10

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

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

11.16.1 לעבוד עם הכלים הקיימים ברשת מכבי.

11.16.2 לעבוד בתשתיות ה-DevOps הקיימות של מכבי.

11.16.3 להורדת כלים נוספים יש לקבל אישור אבטחת מידע.

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

11.16.5 סביבות הפיתוח לא יהיו נגישות בשום אופן לרשת האינטרנט.

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

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

עליה לייצור.

- 11.17.2 כל תהליך שינוי במערכת הכולל שינוי בקוד מחויב לעבור תהליך של Code Review לצורך מזעור סיכוני אבטחת מידע כתוצאה מטעויות בקוד.
- 11.17.3 אפליקציות ותשתיות המערכת מחויבות להיות מוקשחות בהתאם לסטנדרטים המקובלים בשוק.
- 11.17.4 חל איסור לבצע שימוש במידע חסוי/חסוי ביותר/ מידע אישי מזהה כ Test Data בתהליכי QA ופיתוח. לתהליכים אלו יש להשתמש ב Data אנונימי או ב Data רנדומלי בלבד
- 11.17.5 חריגה מאופשרת באישור מראש על ידי מכבי שירותי בריאות.
- 11.18 יש לבצע מבדקי חדירות לפני עלייה לאוויר:
- 11.18.1 יוגדרו לבדיקה משתמשים וסביבה לביצוע הבדיקה.
- 11.18.2 לאחר הבדיקה יפורסם דוח ממצאים.
- 11.18.3 לאחר ישיבת תיקוף יש לטפל בממצאים ברמה גבוהה ובינונית.
- 11.18.4 לאחר הטיפול בממצאים יש לבצע בדיקת חדירות חוזרת.
- 11.18.5 העלייה לאוויר מאושרת לאחר שכל הממצאים הגבוהים/בינוניים טופלו.
- 11.19 אבטחת מידע בענן:**
- במקרה שבמהלך מתן השירותים למכבי יוחזק מידע של מכבי בשירותי ענן, מחויב הספק לפעול כדלקמן:
- 11.19.1 ההתקשרות תאושר רק לאחר אישור "ועדת ענן ארגונית" של מכבי.
- 11.19.2 ספק הענן יהיה ב- EU Region בלבד
- 11.19.3 ספק שירותי הענן יגדיר איש קשר לנושאי אבטחת מידע(בקורות ואירועים).
- 11.19.4 ספק שירותי ידווח על כל חשש או אירוע מהותי בנושא אבטחת מידע וסייבר.
- 11.19.5 ספק הענן יודיע לארגון – ודרכו גם למכבי – על כל דרישה של הרשויות למסירה/עיון במידע של מכבי או לקוחותיה.
- 11.19.6 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.
- 11.19.7 העברת מידע לשירות הענן תבוצע לאחר חתימת הספק על הסכם סודיות.
- 11.19.8 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.
- 11.19.9 הספק מתחייב להודיע למנהל אבטחת המידע ב- מכבי על כל פעילות של העברת מידע של מכבי ומבטחיה לשירותי ענן.
- 11.19.10 על שירות הענן לעמוד בכללי הרגולציה והתקינות הרלוונטיות למכבי על פי צורך והמידע הפעיל בשירות מועבר, מועבד או מאוחסן: PCI, ISO-27001, ISO-27017, ISO 27799, חוק הגנת הפרטיות.
- 11.19.11 ניהול זהויות והרשאות בענן:
- 11.19.11.1 גישה לשירות (הן ניהולית והן מצד לקוח) תבצע במשתמש אישי בלבד.

- 11.19.11.2 בשירות יוגדר פרופיל ההזדהות בהתאם למדיניות הארגון (חוזק סיסמה, נעילה לאחר כניסות שגויות, ניתוק לאחר אי שימוש וכו').
- 11.19.11.3 ההזדהות תבוצע באמצעות SAML בלבד. על הספק לחסום כל אפשרויות הזדהויות אחרות.
- 11.19.11.4 גישה משתמשים תעבור דרך מערכת Proxy של מכבי.
- 11.19.11.5 ההזדהות תתאפשר מכתובות IP של מכבי בלבד.
- 11.19.12 אחסון מידע
- 11.19.12.1 נתוני מכבי ימחקו מהתקני המחשוב בהם משתמש הספק לאחר סיום השימוש בהם או בתום השירות, הראשון מבניהם.
- 11.19.12.2 על פי צורך, תתאפשר לארגון יכולת למחיקה מוחלטת של המידע מהשירות.
- 11.19.13 הצפנת המידע
- 11.19.13.1 נתונים המוגדרים כרגישים (ובכל מקרה במידע רפואי של לקוחות) יוצפנו באחסון.
- 11.19.13.2 ההצפנה תבוצע בהתאם לסטנדרטים המקובלים בשוק.
- 11.19.13.3 מפתחות ההצפנה יישמרו באופן בלעדי בידי הארגון במידת האפשר.
- 11.19.14 ניטור אירועים
- 11.19.14.1 ניטור אירועים על פי המוגדר בסעיף ניטור אירועים
- 11.19.15 העברת מידע
- 11.19.15.1 העברת המידע תבוצע בתווך מזוהה ומוצפן.
- 11.19.16 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.
- 11.19.17 כל מידע המגיע לידי הספק ומי מטעמו יישמר ולא יעשה בו שימוש שלא לצורך הפעילות מול מכבי.
- 11.19.18 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.
- 11.19.19 הספק מתחייב כי כל ספקי המשנה שלו עומדים בכל דרישות אבטחת המידע במסמך זה.
- 11.19.20 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.
- 11.19.21 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.
- 11.19.22 הספק אחראי להתאים את רמת אבטחת המידע שלו לסטנדרטים המקובלים בשוק.