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

שירותי הבריאות הטובים בישראל

12.02.2024

"קול קורא" לחברות לאספקת שירות שילוח תרופות לבית המטופל עבור חברי מכבי

1. מכבי שירותי בריאות (להלן "**מכבי**") מעוניינת להתקשר עם כל חברה המסוגלת לספק **שירותי שילוח תרופות עד לבית המטופל** בהתאם לדרישות החוק ולדרישות הסף של מכבי כפי שיפורטו בהמשך (להלן "**השירות**").
2. חברות העונות על הדרישות כמפורט בסעיף 6 מצ"ב, יגישו את הצעתן, תוך התייחסות מפורטת לעמידה בכל אחת מסעיפי הדרישות, **לשחר מסר בכתובת המייל** messer_s@mac.org.il לא יאוחר מתאריך 27.02.2024 (להלן "**ההצעה**"). ההצעה תכלול התייחסות גם למודל התמחור של השירות המוצע . במידה וההצעה לא תהיה מלאה מכבי תבקש מהחברה השלמות מסמכים והתייחסויות.
3. לאחר בחינת עמידת ההצעה בדרישות הסף, ע"י הגורם המקצועי, ורק לאחר אישורו, יוזמנו נציגי החברה לפגישה במחלקת הרכש לטובת מו"מ.
4. אין בהגשת ההצעה להבטיח התחייבות מכבי להתקשרות עם החברה. מכבי תתקשר עם כל ספק שיעמוד בדרישות, וייתן הצעת מחיר שעליה תהיה הסכמה.
5. בתום המו"מ ייחתם הסכם משפטי עם הספקים שעמדו בכל הדרישות . בנוסף כל ספק יהיה חייב לחתום על הסכם האיכות - **בנספח ב'** מצ"ב.
6. מצ"ב **רשימת הדרישות**:
   - 6.1. **היקף השירות הנדרש:** יכולת אספקת 500 משלוחים לבית המטופל ליום.
   - 6.2. **ניסיון הספק:** 3 שנות ניסיון במשלוח תרופות עד הבית.
   - 6.3. **צי רכבים:** מינימום 15 כלי רכב מיועדים לשינוע תרופות, כלי הרכב צריכים להיות ולידיים, מנוטרי טמפרטורה באופן רציף ומתועד וגם עם יכולת לשאת משלוחים בקירור עד בית הלקוח
   - 6.4. **SLA:** מסירת ההזמנה לבית החבר תתבצע תוך יום עסקים אחד מיום שידור ההזמנה לחברת השילוח ע"י בית המרקחת המכין.
   - 6.5. **דרישות מקצועיות:** עמידה בנהלים 126,128 ו 130 למשרד הבריאות.
   - 6.6. **דרישות מערכות מידע:** דרישות תשתיתיות, ממשקים ואבטחת מידע מפורטים בנספח א' מצ"ב.
   - 6.7. לספק צריכה להיות **מערכת POD** (Proof of delivery) למעקב אחר שילוחים, שיקוף סטטוס משלוח בכל עת למכבי ולמזמין.
   - 6.8. לספק צריכה להיות מערכת אשר שומרת את הנתונים אודות סטטוס משלוחים שתהיה זמינה לשימוש מכבי בכל עת.
   - 6.9. **שירות:** לספק צריך להיות מוקד שירות שייתן מענה ישיר לשיחות מצד החברים שהזמינו. שעות הפעילות של המוקד הן לפחות עד השעה 17:00 כל יום.

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

שירותי הבריאות הטובים בישראל

נספח א' - דרישות מערכות מידע

פרק מערכות מידע ואבטחת מידע

מפרט דרישות אבטחת מידע

כללי

הקדמה

מכבי הגדירה את נושא אבטחת המידע ושמירה על הפרטיות כנושא אסטרטגי ובעל חשיבות עליונה, ולפי כך כל ספק הנותן שירותים בנושא המחשוב חייב לעמוד בדרישות המוגדרות בפרק זה. מערכת לניהול בל"מ נועדה לתמוך ביעדיה האסטרטגיים של מכבי ולשפר את רמת המענה לכל הגורמים הדרושים.

הגדרות

- המזמין – מכבי שירותי בריאות
- מידע - כל מידע (Information), ידע (Know-How), ידיעה, מסמך, תכתובת, תוכנית, נתון, מודל, חוות דעת, מסקנה וכל דבר אחר כיוצ"ב הקשור באספקת השירותים בין בכתב ובין בע"פ ו/או בכל צורה או דרך של שימור ידיעות בצורה חשמלית ו/או אלקטרונית ו/או אופטית ו/או מגנטית ו/או אחרת והכל למעט מידע שהוא נחלת הכלל.
- עובדים – כלל הגורמים המועסקים ע"י הספק לצורך מתן השירותים לרבות קבלני משנה.
- ספק - הספק עימו התקשר המזמין לביצוע השירותים.
- רשת המזמין – אחת מרשתות מערכות המידע המשמשות את המזמין.

התחייבות הספק

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
הספק מצהיר בזאת שידוע לו כי המידע שיתקבל במהלך מתן השירותים אליו או למי מטעמו הוא בעל רגישות מיוחדת	
והוא מתחייב כי הוא או מי מטעמו לא יעבירו מידע זה לכל גורם אחר שבו או עימו הוא קשור שלא לצורך מתן השירותים	
אלא אם כן ניתן לכך אישורו המוקדם של המזמין ובתנאים כפי שייקבעו על ידו.	
הספק מתחייב לפעול על פי הוראות המזמין בכל הקשור לשמירת הסודיות	
ובכלל זה להסדרת אבטחת המידע ונוהלי הגישה למידע, לאיסוף, לסימון, לאימות ולעיבוד הנתונים;	
הספק מצהיר, כי הוא מכיר את הוראות חוק הגנת הפרטיות, התשמ"א-1981, והתקנות שהותקנו על פיו, וכי יפעל כמתחייב מחוק זה ומכל חיקוק אחר הנוגע לשמירתו וסודיותו של המידע שימצא ברשותו.	
מכבי באמצעות מחלקת אבטחת המידע רשאית למסור הנחיות נוספות בנושא שמירה על סודיות ואבטחת מידע במהלך תקופת ההתקשרות בכתב או בעל פה, ויחייבו את הספק ללא יכולת ערעור מצד הספק.	

מידע הנוגע לפרויקט לא ייחשף לשום גורם מחוץ למכבי המזמין ללא אישור בכתב ממכבי.	
הספק מתחייב כי לא יוציא מידע מאתר המזמין ו/או מרשת המזמין בכל אופן פיזי ודיגיטלי ללא קבלת אישור בכתב ממכבי.	

הנחיות אבטחת מידע

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
אופי הפעילות מכבי שירותי בריאות מחייב דגש מיוחד בנושא אבטחת המידע.	
מכבי שירותי בריאות רואה חשיבות רבה במימוש שיטתי ויעיל של היבטי אבטחת המידע במערכות השונות, ובכלל זה היבטים הקשורים הגנה על מידע ולחוק הגנת הפרטיות התשמ"א-1981.	
הנתונים מתקבלים או מופקים ע"י הספק באמצעות מערכות המידע של מכבי שירותי בריאות או באמצעות מערכות המידע המופעלות ע"י הספק במסגרת הפעילות.	
על הספק לפעול במסגרת המערכת על פי הוראות המצורפות בנספח א' ועפ"י דרישות של הרשות למשפט טכנולוגיה ומידע (רמו"ט) מס' 2/2011 – "שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי" המופיעות באתר שכתובתו: http://www.justice.gov.il/NR/rdonlyres/805B34A2-6D8F-481E-A9B2-BEC934ECDA84/35860/1122011.pdf	
חל איסור מוחלט על הספק לאסוף מידע בדרכים בלתי חוקיות או לעשות שימוש במאגר מידע בלתי חוקיים.	
על הספק חל איסור להעביר לצד ג' כלשהו מידע שיקבל במסגרת ההתקשרות במערכת זה או לעשות כל שימוש במידע שאליו נחשף אגב ביצוע מערכת זה, לכל מטרה אחרת שאינה קשורה באופן ישיר לביצוע התחייבויותיו במסגרת ביצוע מערכת זה.	
במהלך ביצוע הפעילות במערכת הספק מתחייב לדאוג לאבטחת כל החומר שיגיע אליו במסגרת ביצוע פרויקט זה ולהציג למכבי, על פי דרישתה או דרישת מי מטעמו של המכבי, את אמצעי אבטחת החומר.	
הספק יתחייב למנוע גישה למערכות המחשוב (בין אם של המכבי, בין אם של הספק או של כל גורם אחר), בהן נשמר מידע הקשור למתן השירותים על פי מערכת זה, ממי שאינו שותף לפעילות. על הספק להגיש למכבי דיווחים שוטפים בכל הנוגע לאופן ניהול מאגרי המידע ועיבוד המידע במתכונת שתיקבע ע"י המכבי. הספק נדרש לדווח באופן מידי למכבי בתוך 8 שעות ממועד האירוע על כל תקלה בנושא אבטחת המידע לרבות, דליפת מידע או שימוש חורג מההרשאה שניתנה. במקרה זה, על הספק לפעול למניעת דליפת המידע וכל נזק כתוצאה מהתקלה.	

מכבי רשאית, בכל עת, לבדוק את מערכות המידע של הספק. על הספק להעמיד לרשותו ולעיונו של המכבי ו/או נציג מטעמו את כל החומר והמידע שידרשו ע"י המכבי ו/או נציגו, עפ"י שיקול דעתו הבלעדי של מכבי ו/או נציגה.	
בלי לגרוע מכל האמור, רשאים נציגיה המוסמכים של מכבי, לבקר באתרי מתן השירותים ולהתרשם מהם ולהעביר את הערותיהם לנציגיו המוסמכים לעניין מערכת זה של הספק, לדרוש הפסקת עבודתו של כל עובד בפעילות הקשורה למערכת.	
הספק יתחייב לעמוד בדרישות אבטחת המידע שפורטו לעיל ובדרישות לשמירת סודיות המפורטות במערכת זה על נספחיו ובדרישות כפי שיוצגו לו מזמן לזמן על ידי המכבי ו/או מי מטעמו, לעמוד בנהלי המכבי בנוגע לאבטחת מידע ושמירה על מידע מוגן, ובכל הוראה רלוונטית אחרת לרבות הוראות חוק, תקנות, צו, הנחיות הרשות למשפט טכנולוגיה ומידע, והנחיות רשם מאגרי המידע.	
ככל שהספק שומר מידע נוסף כלשהו מעבר למידע אשר הוגדר במפורש על ידי מכבי, עליו לבצע את השמירה ואת ההגנה על המידע בהתאם להוראות החוק, התקנות והנחיות רמו"ט הרלוונטיות, לרבות בנוגע לרישום מאגרים, בהתאם לצורך.	
בתום ההתקשרות על הספק להעביר למכבי את כל המידע שהצטבר במהלך ביצוע הפעילות במערכת זה כל זאת בהתאם להוראות וההנחיות הנ"ל.	

שימוש, אחזקה או ניהול של מאגרי מידע

מלוא המידע המצוי במאגרי המידע של מכבי אשר בידי הספק או שיש לספק גישה אליהם במסגרת ההתקשרות בינו לבין מכבי, הינו בבעלות מכבי על כל המשתמע מכך. הספק מתחייב שכל גישה שלו, או של מי מטעמו, למידע ולמאגר המידע, תתבצע אך ורק בהתאם להוראות מכבי ולמטרות אשר הוגדרו לו על ידי מכבי במסגרת ההתקשרות.

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
הספק מתחייב שהוא, או מי מטעמו, יקפיד כי כל איסוף מידע או שימוש בו יבוצע אך ורק בהתאם להוראות החוק והדין, ועל פי הנחיות מכבי.	
הספק מתחייב שהוא, או מי מטעמו, לא יעביר מידע או חלק ממידע, מתוך מאגרי מכבי אשר בידיו או שיש לו גישה אליהם, לצד שלישי ללא אישור מפורש ובכתב מאת מכבי.	
הספק מתחייב שלא לשמור ולא להוציא מידע של מכבי אל שרתים או משאבי מחשוב אחרים הממוקמים מחוץ לגבולות מדינת ישראל, או שונים מאלה אשר נקבעו במסגרת המערכת או ההתקשרות.	

ניהול אבטחת מידע ארגונית

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
הספק מתחייב למנות ממונה אבטחת מידע מטעמו, ואשר יהיה אחראי על אבטחת המידע הנכלל במאגרי המידע המצויים בידי הספק וכן על יישום ההנחיות המופיעות במסמך זה.	
הספק יחתום על התחייבות לשמירת סודיות, וכן יחתים על התחייבות זו את עובדיו ו/או כל מי מטעמו אשר יהיה בעל גישה למאגר מידע של מכבי או למידע מתוכו במסגרת ההתקשרות.	
בכל מקרה שבו לספק התקשרות עם צד שלישי כלשהו אשר יש לו נגיעה בהקשר להתקשרות בין הספק למכבי במסגרת מערכת זה ו/או על יישום ההנחיות המפורטות במסמך זה, הספק מתחייב להודיע על כך למכבי ולפעול על פי הנחיותיו וכן ליידע את הצד השלישי בדבר קיום החובות הנובעות מקיום ההנחיות המפורטות במסמך זה.	
הספק יהיה אחראי כלפי מכבי על כל פעילות עובדיו ו/או מי מטעמו במסגרת ההתקשרות.	
הספק מתחייב למנוע מקרים בהם עובדיו ו/או מי מטעמו ינסו לבצע גישות למאגרים אליהם לא קיבלו הרשאה. במקרה בו עובד ו/או מי מטעם הספק ניסה בפעם השלישית לבצע גישה למאגר שאינו מורשה גישה אליו, על הספק למנוע מהנ"ל כל גישה למאגרי מכבי ולדווח על כך מידית למכבי.	

במידה והתגלו ליקויים בעבודת הספק, או כתוצאה מגילוי חשיפת אבטחת מידע חדשה, הספק מתחייב לעדכן את נוהלי העבודה ולדווח למכבי באופן מידי.	

תיעוד ובקרה

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
הספק מתחייב לנהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת על מערכות שניגשות למאגרי מידע של מכבי .	
הספק מתחייב שבכל פניה למערכת ולרשומות במאגר יירשמו כל הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, והאם הגישה אושרה או נדחתה.	
הספק מתחייב לשמור את נתוני הרישום של מנגנון הבקרה למשך 24 חודשים לפחות.	
באחריות הקבלן לבצע בקרות מתאימות על מנת לזהות ניסיונות פריצה או גישה בלתי מורשית למערכת.	
על הספק לבצע תיעוד של כל אירוע אשר יש בו משום פגיעה בשלמות סודיות וזמינות המידע.	
כל אירוע אבטחה, יחקר וייבדק ויופק דוח אירוע המתאר את הגורמים לאירוע ואת דרכי הטיפול באירוע. הספק יוציא הנחיות לביצוע על מנת להפחית את הסיכוי לאירוע דומה.	
על הספק להכין הוראות להתמודדות עם אירועי אבטחת מידע אשר מתייחסים לחומרת האירוע ולמידת רגישות המידע. בהוראות אלו תהיה התייחסות לצעדים מידיים הנדרשים לטיפול באירוע כגון דיווח למכבי , ביטול הרשאות וכדומה.	
המערכת תותקן בהתאם לנוהל הקמת מערכת הקיים במכבי.	

תמיכה מרחוק

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
גישה מרחוק תתאפשר באמצעות משתמש ייעודי לכל נותן שירות מיקור חוץ ובתיאום מראש עם מכבי לאופן ההתקשרות ותדירותה.	
גישה מרחוק תתאפשר לזמן מוגבל על פי סוג הפעילות אותה יבצע נותן שירות מיקור החוץ.	
מכבי יישם הזדהות חזקה לצורך כל גישה מרחוק של נותן שירות מיקור חוץ.	
מכבי תיישם הצפנה מקצה לקצה לכל אורך נתיב ההתקשרות מרחוק.	
מכבי תנטר כל פעילות שבוצעה בגישה מרחוק.	
חשיפת נותן שירות מיקור חוץ למידע אודות לקוחות תצומצם עד למינימום הכרחי, ובמידת האפשר תחסם במלואה.	

בקרת גישה - מערכות מידע שבהן מטופל מידע מכבי נדרשות לתמוך בבקרת גישה מבוססת תפקיד המסוגלות למפות כל משתמש לאחד או יותר תפקידים וכל תפקיד לאחד או יותר פונקציות מערכת.	
הצפנת תווך - גישה למידע רפואי ע"י צד שלישי, המאפשר עיבודו, אחסונו או העברתו, מחייב שילוב דרישות אבטחת מידע בתווך התקשורת, ובתשתיות מערכותיהם.	

הצפנה

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
בעת יישום מערכות מידע במחשוב ענן, תיושם הצפנה הן באחסון והן בתווך על נתונים רגישים: - נתונים רגישים וחסויים (על פי הגדרת מחלקת אבטחת המידע). - נתוני זיהוי של רכיבי תוכנה שונים, כגון נתוני הזיהוי של שרת האפליקציה לשרת בסיס הנתונים (למען הסר ספק , לא יבוצע שימוש בסיסמה שאינה מוצפנת). - אתר אינטרנט או אפליקציה.	
יש להשתמש במנגנוני הצפנה מוכרים ובדוקים ובהצפנות מקובלות כיום בשוק, ולהימנע בפיתוח אלגוריתם הצפנה ייחודי למערכת. במנגנון הצפנה חדש אשר לא מומש כראוי עלולה להיווצר פרצת אבטחה מפתח ההצפנה יישמר במקום מאובטח בתוך רשת מכבי.	

הזדהות וניהול הרשאות

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
הזדהות לשירותים המותקנים במחשוב ענן יתבססו ככל הניתן על לוגיקת ההזדהות המיושמת במכבי- כאשר מערכות ההזדהות במכבי ישרתו כ Identity Provider.	
על מערכות מחשוב הענן לתמוך בפרוטוקולי הזדהות: OAUTH , SAML2 ו Federation.	
הערה - חל איסור לבצע שימוש בפרוטוקול LDAP משרות הענן באופן ישיר למכבי.	
כל שימוש בשירות ענן ע"י משתמש אנושי מחוץ לגבולות מכבי, הזדהות מול ממשקים אדמיניסטרטיביים ושירותים רגישים יבוצעו באמצעות 2Factor Authentication.	
ארכיטקטורת המערכת תיבנה בצורה מאובטחת ע"ב עקרון הפרדת השרתים בארכיטקטורת Tier-3 ומעלה (Browser, Application Server, Database).	
כל שעוני המערכת בכלל הרכיבים ברשת הספק יסונכרנו באמצעות מקור חיצוני זהה באופן המאפשר שחזור ואיתור אירועי אבטחת מידע מדויקים על פי זמן	
יש ליישם מערכות הגנה לנקודות הכניסה לסביבת הענן במכבי. הרכיבים יוגדרו ע"י תשתיות אבטחת מידע.	

תשתיות מחשוב ענן

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
תשתיות הספק מוגדרות ומוקשחות בהתאם למסמכי Best Practice רלוונטיים לכל סוג תשתית, מערכות הפעלה, ציוד תקשורת, מערכות תומכות, מערכות אבטחת מידע וכל רכיב נוסף ברשת בהתאם להוראות יצרן ותקן CIS	

בקרות

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
אירועי אבטחת מידע - במערכות טכנולוגיית המידע ישולבו אמצעים לגילוי, מניעה, תיעוד, התאוששות והגנה מפני קוד זדוני בתחנות הקצה, בשרתים ובשערי הארגון או עפ"י ארכיטקטורה מתאימה עפ"י החלטת הארגון, כמו כן יש להגדיר נוהל טיפול במקרה של כשל אבטחתי במערכות.	
גישה ליצירת, עדכון או ארכוב מידע תייצר במקביל רשומת בקרה מאובטחת שתזהה יחידנית את המשתמש, את הרשומה את סוג הפעילות שביצע המשתמש ותתעד את הזמן (תאריך, שעה) שבה הפעולה בוצעה ורכיב טכנולוגיית המידע שבו נעשה שימוש.	
ניטור רשומות הלוג Audit Trail יבוצע באופן סדיר.	
שיח לא פעיל יופסק לאחר פרק זמן מוגדר של אי פעילות שיותאם למיקום תחנת העבודה ולפעילות המתבצעת באמצעותה.	
ככל שהדבר רלוונטי, מעגל הגנה ראשון לרכיבי טכנולוגיית המידע יהיה מעגל אבטחה פיזי.	
יש לערב את צוות אבטחת מידע משלב הייזום של הפרויקט ועד להטמעתו. מערכת לא תעלה לאוויר ו/או תבוצע אינטגרציה ללא אישור מפורש של מנהל אבטחת מידע בארגון. במידת הצורך ידרש סקר אבטחת מידע של גורם אחר לאיתור חורי אבטחת מידע ויהיה צורך לטפל בממצאים על פי ההמלצות.	

אבטחת מידע לוגית

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
במקרה שבמהלך מתן השירותים ל-מכבי החברה או מי מטעמה יחזיק מידע של מכבי על אמצעי מחשוב נייח או נייד שאינו ברשת המחשוב של מכבי, אזי תפעל החברה כאמור בסעיפים להלן:	

במידה והחברה מעבדת מידע עבור מכבי המסווג כ"רגיש" 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 של מכבי. למען הסר ספק, ניתן לקשר את מחשבי החברה (אשר אינם משמשים לאחסון המידע של מכבי לרשת האינטרנט.	
החברה תיישם מידור פנימי בגישה לקבצים המכילים מידע של מכבי. הגישה לקבצים אלה תתאפשר רק למי שעבודתם ותפקידם בחברה מחייבים זאת, ולמכביו שחתמו על הסכם סודיות מול חברת מכבי.	
החברה תוודא הצפנה של קבצים המכילים מידע של מכבי המסווג כ"רגיש" ע"פ מדיניות סיווג המידע של מכבי.	
קבצים המכילים מידע של מכבי המסווג כ"רגיש" ע"פ מדיניות סיווג המידע של מכבי, יועברו אל ומהחברה אל ומ-מכבי באופן מוצפן.	
אין להעביר קבצים המכילים מידע של מכבי בדוא"ל ו/או בכל אמצעי תקשורת אחר לגורמים אחרים ללא אישור כתוב מ-מכבי.	
לא יבוצע שימוש להעברת קבצים ושיתוף מסמכים דרך שירותים מסחריים חיצוניים כגון Google docs, jumbo mail וכו'.	
בתחנות העבודה של החברה תשמר אבטחת המידע באופן הבא:	
לא ישמרו קבצי מכבי על הדיסק הקשיח של התחנה (למעט לגבי חברה או יחיד ללא רשת משתמשים).	
הכניסה לתחנה תהיה באמצעות USER ID וסיסמא אישית.	
אורך הסיסמא יהיה לפחות שבעה תווים.	

שימוש ברכיבי אבטחת מידע

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
הספק יעשה שימוש ברכיבי אבטחת המידע הבאים, לכל הפחות:	
- התקניfirewall , שישמשו לחציצה בין רשתות בסיווגים שונים, להגנת הממשקים.	
- התקני WAF, להגנת אתרי WEB.	
- firewall XML להגנת הממשקים מול מכבי.	
- התקני IPS ,להגנת הקישור לרשת ה-Internet.	
- התקני DLP , למניעת הוצאת מידע שאיננו מאובטח אל מחוץ לרשת.	
הספק יעשה שימוש ברכיבי אבטחת המידע הבאים, לכל הפחות:	
- התקני firewall ,שישמשו לחציצה בין רשתות בסיווגים שונים, להגנת הממשקים.	
- התקני WAF ,להגנת אתרי WEB.	
- תוכנות אנטי-וירוס, לכלל העמדות והשרתים ברשת.	
- מערכתNAC , למניעת גישה בלתי מורשת לרשתות הספק.	

אבטחת מידע בתנועה

דרישה	הערות הספק (עומד/לא עומד) במידה ולא עומד יש להסביר
הספק נדרש להעביר מידע אשר נמצא בתנועה כגון מידע העובר בין המערכות המרכזיות למערכות המפעיל, ובין מערכות המפעיל ליישום הסלולרי, על גבי תווך תקשורת מוצפן לפחות אחד מאלה: .)'וכו SSL/IPSEC/VPN/SSH(המפעיל יידרש לאבטח את המערכות על ידי אמצעים להגנה מפני מתקפות מסוג DDOS תשתיתי ואפליקטיבי. המפעיל יספק פתרון אבטחה מתקדם המספק יכולות מתקדמות של ניטור ובקרה, מניעת פעילות זדונית בזמן הזיהוי, הצפנה במנוחה/תנועה, יכולות תיעוד ומעקב אחר פעולות ושינויים ויכולות אבטחה נוספות הנכללות בפלטפורמה זו.	

1.1.הנחיות אבטחת מידע – פתרון ענני

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

למען הסר ספק הפניה לבודק, 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.

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

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

1.1.6.במקרים שבהם הספק מקבל ממכבי מידע המכיל פרטים אודות חברי מכבי ו/ואו עובדיה, הספק מצהיר כי הוא פועל כנדרש על פי חוק הגנת הפרטיות התשמ"א-1981, התקנות מכוחו והנחיות הרשות להגנת הפרטיות במשרד המשפטים (להלן ביחד: "החוק"), וכי הוא נוקט באמצעי אבטחה ובקרה כמתחייב מהחוק.

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

1.2.1.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).

1.2.3.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 ו/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 בארונית, 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 מידע 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 שמשתמש זה יפעל כאמור בסעיפים שלהלן, מכל אתר ומכל מחשב ממנו יתחבר לרשת מכבי:

1.4.1. 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.

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:

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.ארכיטקטורה

1.6.1.האתרים יהיו תחת Domain מכבי (כלומר הURL של האתרים יהיו בDomain מכבי).

1.6.2.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.

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

1.6.4.שליחת המיילים יועברו מכתובת של מכבי בלבד. לצורך כך הספק מתחייב להעביר כתובות IP למכבי לצורך הגדרת SPF.

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

1.6.6.הספק יישם את הגדרות האבטחה הבאות:

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

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

1.6.6.3.כל הנתונים ישמרו מחוץ לשרת ה WEB בשרת מסד הנתונים ייעודי .

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

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

1.6.6.6.עובדים פנימיים יזדהו למערכת על בסיס SSO (הזדהות מכבי)

1.6.7.בכל אתר / פלטפורמה שמזוהה בשם מכבי יש לשלב את דרישות הארכיטקטורה הבאות:

1.6.7.1.תבוצע הפרדה בין שרתי מכבי לשרתי הספק ושרתי לקוחות נוספים. ההפרדה תבוצע לבאים: שרת זהויות, מסדי נתונים, שרתי WEB ואפליקציה.

1.6.7.2.שרת מסד הנתונים ושרת הזהויות, ישבו בסגמנט ייעודי מופרד ב FW מסגמנט שרת ה WEB . סיגמנט זה יהיה חסום לגישה אל ומ – האינטרנט.

1.6.7.3.תבוצע הפרדה בין סביבת הייצור לסביבת הפיתוח והבדיקות. ההפרדה תבוצע הן ברמת אפליקציה והן ברמת תשתיות (שרת וב, שרת מסד נתונים וכו').

1.6.7.4.יוגדרו סיגמנטים ייעודיים עבור שרתי מכבי אשר יופרדו מבחינת תקשורת משאר שרתי הספק (הכוונה למערכות ההפעלה, ולא לברזלים המחזיקים את כלל השרתים הווירטואליים).

1.6.7.5.ההזדהות של עובדי מכבי לשירות תבוצע באמצעות SAML

1.6.7.6.באתרים יופעלו שירותי\מערכות הבקרה הבאים (השירותים\מערכות יופעלו במוד הגנה אקטיבית (חסימה) ולא במוד למידה):

1.6.7.6.1.FW – אפיון והגדרה של ה WAF באופן אקטיבי על בסיס התאמה לאתר האינטרנט.

1.6.7.6.2.IPS

1.6.7.6.3.ממשק הפלטפורמה ל- WAF של מכבי

1.6.7.6.4.Anti DOS\DDOS (להגנה ספציפית על אתרי מכבי).

1.6.7.6.5.אנטי וירוס - האנטי וירוס יעודכן ברמה יומית.

1.6.7.6.6.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.

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

1.6.7.7.מועמדים חיצוניים (שאינם עובדי מכבי) יזדהו למערכת באמצעות חשבון אישי באתר.

1.6.7.8.הזדהות עובדי מכבי ב SSO בלבד.

1.7.ממשקי Web Service

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

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

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

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

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

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

1.8.הצפנה

1.8.1.דרישות תעודת הצפנה:

1.8.1.1.תעודת הספק תהיה מ issuer חיצוני ולא CA מקומי

1.8.1.2.אלגוריתם של התעודה תהיה sha256

1.8.1.3.התעודה תכיל CRL Distribution Points

1.8.2.דרישות לגבי ההצפנה:

1.8.2.1.העבודה מול הספק תהיה בתווך TLS ver. 1.2 or above

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

1.9.ניטור אירועים

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

1.9.2.לוג האירועים יוגדר על הבאים:

1.9.2.1.בכל מודול ומערכת שמאחסנת מידע של מכבי.

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

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

1.9.3.לוג אירועים יופעל על האירועים הבאים:

1.9.3.1.כניסות למערכת – מוצלחות או כישלונות.

1.9.3.2.כל גישה לנתונים, כולל קריאה בלבד.

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

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

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

1.9.4.רישום כל אירוע יכלול את הערכים הבאים:

1.9.4.1.מועד ביצוע הפעולה.

1.9.4.2.שם משתמש מבצע הפעולה.

1.9.4.3.כתובת מקור.

1.9.4.4.סוג ה – Client.

1.9.4.5.שם הפעולה.

1.9.4.6.סטטוס – הצלחה\כישלון.

1.9.4.7.תיאור הפעולה.

1.10.פיתוח

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

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

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

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

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

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

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

1.10.7. חל איסור לבצע שימוש במידע חסוי/חסוי ביותר/ מידע אישי מזוהה כTest Data בתהליכי QA ופיתוח. לתהליכים אלו יש להשתמש בData אנונימי או בData רנדומלי בלבד

1.10.8. חריגה מאופשרת באישור מראש על ידי מכבי שירותי בריאות

1.11. אבטחת מידע בענן:

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

1.11.1. ההתקשרות תאושר רק לאחר אישור "ועדת ענן ארגונית" של מכבי.

1.11.2. ספק הענן יהיה ב- EU Region בלבד

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

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

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

1.11.6. 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.

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

1.11.8. 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.

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

1.11.10.על שירות הענן לעמוד בכללי הרגולציה והתקינות הרלוונטיות למכבי על פי צורך והמידע הפעיל בשירות מועבר, מועבד או מאוחסן: ISO 27799, ISO-27001, ISO-27017, PCI , חוק הגנת הפרטיות.

1.11.11.**ניהול זהויות והרשאות בענן:**

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

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

1.11.11.3.ההזדהות תבוצע באמצעות SAML בלבד. על הספק לחסום כל אפשרויות הזדהויות אחרות.

1.11.11.4.ההזדהות תתאפשר מכתובות IP של מכבי בלבד.

1.11.12.**אחסון מידע**

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

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

1.11.13.**הצפנת המידע**

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

1.11.13.2.ההצפנה תבוצע בהתאם לסטנדרטים המקובלים בשוק.

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

1.11.14.**ניטור אירועים**

1.11.14.1.ניטור אירועים על פי המוגדר בסעיף ניטור אירועים

1.11.15.**העברת מידע**

1.11.15.1.העברת המידע תבוצע בתווך מזוהה ומוצפן.

1.11.16.

1.11.17.הספק מתחייב להחתים את עובדי ושלוחיו הרלוונטיים על הצהרות סודיות, הכוללות, בין היתר, התחייבות לשמירה מוחלטת על סודיות המידע של מכבי. למען הסר ספק, ניתן לבצע שימוש בנוסח ההתחייבות לשמירת סודיות המקובל אצל הספק.

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

1.11.19.כל מידע שייחשף במסגרת מתן השירותים הנוגע למכבי ו/או לחבריה ו/או לעובדיה לא יועבר לצד ג' ללא אישור בכתב ממנהל אבטחת המידע והגנת הסייבר במכבי.

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

1.11.21.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.

1.11.22.אין בהתחייבות הספק במסמך זה כדי לגרוע או להפחית מאחריותו של כל עובד שלו לגבי דרישות מסמך זה ו/או לאחריות הספק למילוי הוראותיו ע"י כל עובדיו ושלוחיו.

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

1.12.אבטחת מסמכים

1.12.1.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.

1.12.2.מסמכים המכילים מידע של מכבי ישמרו נעולים בארונית, מגירה, ארון או כספת שהוקצו לצורך זה בלבד.

1.12.3.הגישה למסמכים אילו תותר רק למי שעבודתם ותפקידם אצל הספק מחייבים זאת, ולכאלו שחתמו על התחייבות לשמירת סודיות מול מכבי.

1.12.4.אין להעביר מסמכים המכילים חומר מודפס של מכבי לגורמים אחרים בכל אמצעי (פקס, דואר ישראל וכו'), ללא אישור כתוב ממכבי.

1.12.5.אין להשאיר מסמכים עם חומר של מכבי על השולחן/במדפסת בסוף יום העבודה.

1.12.6.יש לגרוס מסמכים המכילים מידע של מכבי בתום השימוש בהם.

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

1.13.הנחיות אבטחת מידע לפתרון on-prem

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

1.13.2.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.

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

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

1.13.5.במקרים שבהם הספק מקבל ממכבי מידע המכיל פרטים אודות חברי מכבי ו/ואו עובדיה, הספק מצהיר כי הוא פועל כנדרש על פי חוק הגנת הפרטיות התשמ"א-1981, התקנות מכוחו והנחיות הרשות להגנת הפרטיות במשרד המשפטים (להלן ביחד: "החוק"), וכי הוא נוקט באמצעי אבטחה ובקרה כמתחייב מהחוק.

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

1.14.1.הגדרות

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

1.14.1.2.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

1.14.2.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).

1.14.3.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.

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

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

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

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

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

1.14.7.2.הכניסה לתחנה תהיה באמצעות USER ID וסיסמא אישית.

1.14.7.3.אורך הסיסמא יהיה לפחות שבעה תווים.

1.14.7.4.הסיסמאות יוחלפו כל שלושה חודשים לפחות.

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

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

1.14.7.7.תותקן תכנת הגנה תקנית ומעודכנת כנגד וירוסים.

1.14.7.8.מערכת ההפעלה המותקנת על התחנה מעודכנת בעדכוני האבטחה האחרונים שהופצו על ידי היצרן.

1.14.8.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.

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

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

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

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

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

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

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

1.14.14.2.יבוצע שימוש בפרוטוקול WPA 2.

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

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

1.14.15.2.יוגדר לוג אירועים על השימוש בשירות.

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

1.15.אבטחת מסמכים

1.15.1.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.

1.15.2.מסמכים המכילים מידע של מכבי ישמרו נעולים בארונית, מגירה, ארון או כספת שהוקצו לצורך זה בלבד.

1.15.3.הגישה למסמכים אילו תותר רק למי שעבודתם ותפקידם אצל הספק מחייבים זאת, ולכאלו שחתמו על התחייבות לשמירת סודיות מול מכבי.

1.15.4.אין להעביר מסמכים המכילים חומר מודפס של מכבי לגורמים אחרים בכל אמצעי (פקס, דואר ישראל וכו'), ללא אישור כתוב ממכבי.

1.15.5.אין להשאיר מסמכים עם חומר של מכבי על השולחן/במדפסת בסוף יום העבודה.

1.15.6.יש לגרוס מסמכים המכילים מידע של מכבי בתום השימוש בהם.

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

1.16.גישה לרשת ולמערכות מכבי

במקרה ובמהלך מתן השירותים למכבי יוקצה למי מטעם הספק שם משתמש לרשת ולמערכות מכבי הספק אחראי לכך שמשתמש זה יפעל כאמור בסעיפים שלהלן, מכל אתר ומכל מחשב ממנו יתחבר לרשת מכבי:

1.16.1. 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.

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

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

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

1.16.5. 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 .

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

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

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

1.17. שימוש באמצעי mobile ומחשבים ניידים:

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

1.17.1. 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.

1.17.2. 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.

1.17.3. 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.

1.17.4. 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.

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

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

שירותי הבריאות הטובים בישראל

נספח ב'

הסכם איכות

שנערך ונחתם ב_____ ביום____ לחודש _____ בשנת _____

בין: חברת _____ (להלן "הספק") לבין: מכבי שירותי בריאות (להלן "הלקוח")

לפיכך הוצהר, הותנה והוסכם בין הצדדים כדלקמן:

הואיל: והספק מנהל ומפעיל בית מסחר לאחסון והפצת תרופות ע"פ דין;

והואיל: והלקוח מעוניין בהובלת ו/או אחסון משלוחים בתנאים מבוקרי טמפרטורה, כמפורט להלן בהסכם זה, באמצעות הספק (להלן: "השירותים");

והואיל: והספק מצהיר ומתחייב כי במשך תקופת ההסכם, יוביל ו/או יאחסן באמצעות בית המסחר, בהתאם להוראות הסכם זה;

והואיל: ועל סמך הצהרת והתחייבות הלקוח והספק כאמור לעיל, מסכים הספק להעמיד לרשות הלקוח כושר הובלה ו/או אחסון, והכל בתנאים כפי שיפורטו להלן בהסכם זה;

והואיל: וברצון הצדדים לגבש ולהעלות על הכתב את התנאים להתקשרותם בהסכם זה;

<u>על כן הוסכם והותנה בין הצדדים כלהלן:</u>

1. **<u>מבוא ונספחים</u>**

1.1. ההסכם האיכות כמפורט במסמך זה, הינו חלק בלתי נפרד מהסיכום העסקי בין מכבי שירותי בריאות לבין _____ בע"מ.

1.2. במידה וקיימת סתירה בין הגדרות ההסכם המסחרי להגדרות הסכם איכות זה, יש לעבוד בהתאם להגדרות הסכם האיכות.

1. **<u>הגדרות איכות</u>**

1.1. <u>GDP- Good Distribution Practice</u> - כלל הפעולות המבוצעות על ידי הספק על מנת להבטיח שמירה על הטובין המאוחסן ומובל על ידו, בהתאם לדרישות היצרן וללא פגיעה משום סוג בתכשיר או באריזתו.

1.2. <u>כיול טמפ'/ לחות</u> - בדיקה תקופתית לדיוק החיווי הניתן על ידי רגשי מערכת המדידה. הכיול יבוצע ע"י מעבדה מוסמכת ע"י הרשות הלאומית להסמכת מעבדות בהתאם לתקן ISO 17025.

1.3. <u>ולידציה</u> - (תיקוף) הוכחה שיטתית ומתועדת המבוססת על ניהול סיכונים לגבי כך שתהליך או ציוד מוגדר, אכן מוביל באופן הדיר לתוצאה הנדרשת.

1.4. ניהול סיכונים - תהליך זיהוי סיכונים הקשורים למוצר, בחינת והערכת הסיכונים, ניהולם ובחינת האפקטיביות של תהליכי הבקרה שהוגדרו. התהליך כולל ניתוח סיכונים, הערכת סיכונים ובקרת סיכונים.

1.5. אירוע חריג – כל אירוע המהווה חריגה מהחוק, תקנות, רגולציה, נהלים ונורמות בארגון שעלול להוביל או הוביל לנזק.

חריגת טמפרטורה- בטווח $15\text{-}25^0C$ חריגה בתחום $25\text{-}30^0C$ ליותר מ30 דקות. כל חריגה מעל 30^0C. חריגה מתחת ל 15^0C למשך 30^0C דקות ויותר. בטווח 2-8 חריגה מעל 8^0C ליותר מ30 דקות עד 20^0C , חריגה מתחת ל2^0C במיידי

2. **<u>התחייבויות מקבל החוזה-</u>**

2.1. מקבל החוזה מתחייב להחזיק בכל הרישיונות הנדרשים והביטוחים כמקובל, לעמוד בתקני האיכות ולספק את התעודות והאישורים הרלוונטיים ללקוח.

2.2. מקבל החוזה מתחייב לשמור על תקינותם של מערכי האחסנה שברשותו, לוודא שאזורי האחסנה ורכבי ההפצה הינם בעלי ולידציה בתוקף ולבצע כיול למערכות הדורשות כיול, כגון מדי טמפרטורה ו/או לחות, בהתאם לדרישות משרד הבריאות לפי עקרונות ה- GDP (Good Distribution Practice) ונהלים מס׳ 128,126 ו-130.

2.3. מקבל החוזה מתחייב לקיים מערך תחזוקה ובדיקה לתקינות מערכות המיזוג והקירור ומערכות הניטור והבקרה אשר מותקנים באזורי האחסון וברכבי ההפצה.

2.4. מקבל החוזה מתחייב לשמור על ניקיון אזורי האחסון ורכבי ההפצה. בנוסף לכך, עליו לתחזק מערך ניטור והדברה למניעת מזיקים על ידי חברה מורשית.

2.5. מבלי לפגוע באמור לעיל, מקבל החוזה מתחייב לאחסן ו/או להפיץ את החבילות בהתאם להוראות כל דין החלים לגביו ובהתאם להנחיות הלקוח, כפי שתהיינה מעת לעת. בפרט, מקבל החוזה מתחייב כי תנאי האחסנה ו/או ההפצה המתבצעים על ידו יבטיחו כי:

- תנאי הטמפרטורה שקבע הלקוח ישמרו, ינוטרו ויתועדו באופן רציף.
- תנאי האחסון ו/או ההפצה לא ישפיעו לרעה על שלמות התכשירים או על איכותם. תכשירים רפואיים לא יזהמו ולא יזוהמו על ידי תכשירים אחרים ו/או על ידי גורמים חיצוניים וסביבתיים.
- ינקטו אמצעי זהירות הולמים למניעת כל דליפה, שבירה או פגימה של הטובין.
- יחול איסור אכילה/שתיה/עישון בסביבת העבודה, פרט לאזורים המיועדים לכך.
- יחול איסור כניסה לאזורי האחסון, לכל אדם שאינו מוגדר כמורשה כניסה על ידי הספק עצמו.
- מקבל החוזה מתחייב להפיץ משלוחים בתנאי אחסון מיוחדים (קירור/ הקפאה) עד טווח הזמן שמאפשר המארז הואלידי בו נארזו. הספק לא יפיץ תכשירים רפואיים באותו רכב עם פריטים העלולים לפגוע באיכות התכשיר כגון מזון, פרחים, קרח יבש וכ׳.
- מקבל החוזה מתחייב לשמור ולהחזיר ללקוח את כל הציוד אשר יסופק על ידו, בשלמותו, לרבות מארזים ואלידיים ואוגרי טמפרטורה (לוגרים) המלווים את המשלוחים.

- מקבל החוזה מתחייב לשנע את החבילות תמיד באריזתן המקורית, כפי שהועבר אליו על ידי הלקוח. אין להוציא טובין מהאריזה המקורית או מהמארז הואלידי, לרבות החלפה באריזה אחרת, מכל סיבה שהיא, אלא אם כן ניתנה הוראה מפורשת וכתובה על ידי רוקח אחראי מטעם הלקוח.
- מקבל החוזה מתחייב לנהל את המשלוחים המערכת POD התאפשר ניהול בזמן אמת של החבילות והוכחות אספקה.
- בפעילות קרוס דוק המבוצעת מתוך בית מסחר _____, מקבל החוזה יאפשר ללקוח לצפות בנתוני אספקת המשלוחים. במידה ולא יתאפשר, יועברו אישורי אספקה ללקוח.
- במקרה בו המשלוח לא נמסר לנמען, מכל סיבה שהיא, יחזיר הנהג את המשלוח לבית המסחר והלקוח יעודכן על ידי הספק. במקרה בו לא נמסר לנמען משלוח המוגדר בתנאי קירור/הקפאה, יעודכן הלקוח טלפונית באותו היום והספק יפעל על פי הנחיותיו של רוקח אחראי מטעם הלקוח.
- החזרות מלקוחות קצה יבוצעו רק בהנחיית הבטחת איכות מטעם נותן החוזה.

3. **<u>התחייבויות נותן החוזה-</u>**

3.1. הלקוח יעביר כתב מינוי רוקח אחראי, רשיון עסק וכל תעודה רלוונטית שיתבקש.

3.2. בפעילות הפצה דרך בית מסחר _____- נותן החוזה יספק את כל פרטי המשלוח וזאת בהתאם לדרישות הספק המוגדרות במערכת המשלוחים בהתאם ללוחות הזמנים שיקבעו. כל חבילה תסומן בברקוד ייעודי, חד ערכי, וימולאו כל הפרטים הנדרשים במערכת הממוחשבת.

3.3. נותן החוזה ימנה נציג אשר ייתן מענה למקרים חריגים בעת ההפצה.

3.4. מסירת המשלוח נותן החוזה אל מקבל החוזה תתבצע בליווי ניירת מתאימה (רשימת חבילות/ תעודת משלוח וכיוב)

3.5. הלקוח מתחייב לדאוג לסימון החבילות כפי שנדרש על ידי הספק והרגולטור (ציטוטוקסיקה, סמים, תנאי אחסון וכיוב').

3.6. במידה והמשלוח דורש תנאי הובלה מיוחדים (קירור/הקפאה), הלקוח יסמן זאת במדבקה מתאימה על גבי החבילה.

3.7. הלקוח יעביר משלוחי קירור במארזים ואלידיים לפחות ל48 שעות.

3.8. במשלוחים בהם נדרש משטח, הלקוח יכין משטוח תקני אשר יוגדר עפ"י הסטנדרטים להלן:

- משטח תקני - משטח פלסטיק או <u>עץ אשר טופל בחום</u>. לא יתקבלו משטחי עץ שלא טופלו בחום
- שרינק
- חזות כך שכל קרטון מציג את תכולתו כלפי חוץ

- קרטונים שאינם בולטים מן המשטח
- משטחים נקיים

היה והתקבל משטח פגום, מכל סיבה שהיא, באחריות הספק לדווח על כך ללקוח.

3.9. חבילות סמים מסוכנים או במידה והחבילה מחייבת טיפול מיוחד, יסומנו בהתאם הן פיזית והן בשידור הדיגיטלי. באספקת סמים המחייבת איסוף מרשם מקור, נותן החוזה יעביר משימת איסוף יעודית בשידור.

3.10. הלקוח מתחייב להעביר את החבילות ואת השידור בהתאם לשעה שסוכמה בהסכם המסחרי

3.11. במידה ויש צורך באיסוף מלקוח קצה (חבילה או מרשם מקורי), תפתח משימת החזרה יעודית ותשודר עם החבילה למסירה (בהנחה שמתאפשר)

3.12. הלקוח לא יעביר חבילות המכילות פריטים העלולים לפגוע באיכות התכשירים המופצים כגון מזון, פרחים, קרח יבש חומרים מסוכנים וכיוב׳. הלקוח מתחייב לארוז את ההזמנות כך שלא יהוו סיכון עבור החבילות האחרות. חבילות המכילות נוזלים בנפח גדול (מעל 100 ml) יש לארוז בצורה שתמנע פגימת חבילות נוספות במקרי נזק. חבילות המכילות נוזלים בנפח גדול יסומנו בהתאם. במידה וחבילה שהכילה נוזלים שלא נארזו בצורה שתמנע שפך פגמה חבילות נוספות, יחוייב הלקוח בעלויות הנזק לחבילות.

3.13. משלוחים הדורשים תנאי אחסנה בקירור יארזו בשקיות יעודיות ע״י בית המרקחת המנפק ויסומנו בהתאם הן פיזית והן לוגית. איסוף משלוחי קירור ע״י מקבל החוזה יעשה במארזים ואלידיים וישונע בתנאי קירור (מקרר/ מארז קירור ואלידי)

3.14. במידה והספק נדרש להרכיב מארזי קירור של הלקוח, הלקוח עביר לבית המסחר הוראות עבודה רלוונטיות, ואלידציות של המארזים, קרחומים וכל ציוד אחר היאפשר השמשה מיידית של המארזים.

3.15. נותן החוזה יעביר הזמנות המיועדות להפצה ביום העוקב בלבד. נותן החוזה יכין הזמנות לקווי אספקה מיוחדים אשר אינם יוצאים ברמה יומית (כדוגמת אילת) בהתאם ללוחות הזמנים של השילוח.

3.16. מסירה למזמין:

- הנהג יזהה את המזמין ויחתים אותו על קבלת המשלוח באישור מסירה (דיגיטלי/ קשיח)
- באספקת סמים מסוכנים הנהג יזהה את המזמין עד פי תעודה מזהה.
- במידה והמזמין לא נוכח, מסירה תתבצע למיופה כוח בלבד כפי שאופר בשידור הדיגיטלי מראש.
- אספקת תכשירי קירור אשר נארזו במארז וואלידי, תתבצע בפתיחת המארז מול המזמין בלבד.

4. **<u>בקרת טמפרטורה ו/או לחות</u>**

באחריות הספק להתקין בכל אזורי האחסון המיועדים לאחסון מוצרים מבוקרי טמפרטורה, כפי שיוגדרו על ידי הלקוח, אמצעים למדידה ותיעוד טמפרטורה ו/או לחות בזמן האחסנה ו/או ההפצה. כמו כן באחריות הספק לוודא כי יתקיימו התהליכים המפורטים להלן:

4.1. הספק מחזיק בבית מסחר וברכבי הפצה מבוקרי טמפרטורה On-line, הכולל תיעוד טמפרטורה לכל אורך שרשרת ההפצה.

4.2. על מערכות המיזוג בבית המסחר וברכבי ההפצה לפעול בכל עת בזמן אחסון והפצת מטעני הלקוח. במהלך פריקת משלוחים יש לוודא כי פתיחת דלתות הרכב תתקיים בזמן המינימלי.

4.3. במהלך כל שלבי האחסנה, טווח הטמפרטורה באזור האחסנה יהיה בגבול טווח טמפרטורה תקין. טווח טמפרטורה תקין ואופן קבלת וניהול התרעות על ידי גורמי מפתח, יוגדר בהתאם למערכת האיכות של הספק ולהנחיות הלקוח כדלהלן:

- טמפרטורה של $15\text{-}25^{0}C$ באזורי האחסון בבית המסחר וברכבי ההפצה.
- טמפרטורה של $2\text{-}8^{0}C$ במקרר בבית המסחר ובמקררים ברכבי ההפצה.
- 65% RH באזורי האחסון בבית המסחר.

4.4. על פי דרישת הלקוח, יימסר לו תיעוד הטמפרטורה במהלך האחסון ו/או ההפצה.

5. **<u>הבטחת איכות ודיווח</u>**

הספק מתחייב לקיים מערכת בקרת איכות וביקורת פנימית, שתבטיח כי מתקיימים תמיכה ניהולית מספקת, פיקוח, ותשתית ראויה, על מנת לספק שירותים העומדים בהוראות הדין הרלוונטיות לאחסנת והפצת תכשירים פרמצבטיים, מכשור רפואי, מזון רפואי ותוספי מזון ותמרוקים; להבטיח כי עובדיו יהיו מוכשרים, מוסמכים ומיומנים למילוי תפקידם; וכן למנות בעסקו בעל תפקיד המוסמך כאחראי הבטחת איכות. מבלי לגרוע מכלליות האמור –

5.1. הספק מתחייב לתחזק מערכת איכות על פי עקרונות ה-GDP.

5.2. הספק מתחייב לרמה גבוהה של איכות ושירות ללקוח, באופן המאפשר תנאי אחסנה והפצה נאותים, גם בסביבה החיצונית לבית המסחר.

5.3. הספק יתעד ויודיע ללקוח בהקדם האפשרי ועד 24 שעות על כל תקלה ו/או חריגת טמפרטורה הנוגעת באופן ישיר למוצרי הלקוח. הספק מתחייב לקבל את הנחיות הלקוח לגבי אופן הטיפול במוצרים אלו ולפעול בהתאם להן.

5.4. דיווח חריגות הקשורות ישירות למשלוחי הלקוח ידווחו ללקוח עד 48 שעות וסיכום תחקיר ישלח עם 30 ימי עבודה. חריגה מתנאים נאותים בהפצה/ אחסנה תדווח בסמוך לזיהוי הארוע.

5.5. הספק מתחייב לקיים בעסקו נהלי עבודה שיטתיים, שיבטיחו עמידה בתנאי מערכת האיכות, אשר יכללו בין היתר את הנושאים הבאים:

- תיעוד ושמירת מסמכים ורשומות, לרבות ניטור טמפרטורה במהלך האחסנה ו/או ההפצה, לתקופה של 6 שנים לפחות.
- הדרכה ורישוי של עובדים, כולל הגדרות תפקיד ואחריות;
- תחזוקה, ניקיון ומערך הדברה;
- ולידציה וכיול טמפרטורה/ לחות ואמצעי מדידה;
- תלונות איכות ותלונות שירות;
- טיפול בחריגות, CAPA;
- בקרת שינויים;
- ניהול סיכונים;
- תוכנית מבדקים פנימיים;
- אבטחת מתחמי האחסון;
- סקרי הנהלה.

6. **<u>טיפול בתלונות</u>**

כל תלונה שתועבר מהלקוח לספק, תיחקר על ידו וישלח מענה בכתב ללקוח. המענה יישלח בתוך 30 ימי עבודה לכל המאוחר.

7. **<u>החזרה מהשוק - Recall</u>**

בכל מקרה של Recall (החזרת מוצר מהשוק) , הספק והלקוח ישתפו פעולה בכל הנדרש על מנת לבצע את התהליך בדרך היעילה והמהירה ביותר על פי הנהלים המחייבים בחוק. הספק והלקוח אחראים לוודא כי בכל עת ישנו ברשותם נוהל כתוב ומעודכן בנושא זה.

8. **<u>מבדק ספק מטעם הלקוח</u>**

הלקוח יהיה רשאי לבצע מבדקי ספק מעת לעת במתקני בית המסחר, בכפוף לתיאום מוקדם עם מחלקת הבטחת איכות של הספק. בעת הגעת נציגי הלקוח לבית המסחר, באחריותם לפעול בהתאם להנחיות והוראות העבודה והבטיחות באתר.

9. **<u>סודיות</u>**

הספק מחויב לשמור על סודיות בכפוף לדרישות הלקוח. הספק מתחייב כי במסגרת פעילותו השוטפת ובעת ביקורות שיערכו בבית המסחר על ידי צד שלישי, לא תחול פגיעה בדרישות הסודיות של הלקוח.

ולראיה באו הצדדים על החתום :

מכבי פארם	_____
שם:	שם:
תפקיד:	תפקיד:
חתימה:	חתימה:

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

שירותי הבריאות הטובים בישראל

שם :

תפקיד :

חתימה :

שם :

תפקיד :

חתימה :

נספח מס׳ 1

רשימת אנשי קשר

הספק- _____

שם מלא	תפקיד	מייל	טלפון

הלקוח- מכבי פארם

שם מלא	תפקיד	מייל	טלפון