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

מכבי
שירותי הבריאות הטובים בישראל

21.08.2022

בקשה להצעת מחיר לאספקת מערכת בקרה למערכות אבטחת מידע (BAS) במכבי

(להלן – "**הבקשה**")

1. כללי

1.1. מכבי שירותי בריאות (להלן – "**מכבי**"), מעוניינת לקבל הצעות מחיר לאספקת מערכת בקרה למערכות אבטחת מידע (BAS) במכבי והשירותים הנלווים למערכת (להלן- "**המוצרים והשירותים**"), כמפורט בבקשה.

1.2. את ההצעות יש למלא על גבי טופס ההצעה המצורף ולשלוח אל שחר מסר לדואר אלקטרוני messer_s@mac.org.il עד יום 04.09.2022.

1.3. בשאלות טכניות בנוגע לתכולת ההצעה, יש לפנות אל אבישי ויספיש weisfish_a@mac.org.il .

1.4. מכבי אינה מתחייבת לקבל את ההצעה הזולה ביותר, חלק מההצעה או כל הצעה שהיא.

1.5. הצעות שלא עומדות בסף איכותי נדרש יפסלו.

1.6. היות מציע בעל ההצעה הכלכלית המיטבית אינו מבטיח את זכייתו. זכייה תוכרז לאחר שקלול המחיר והאיכות כפי שתחליט מכבי.

1.7. מכבי שומרת לעצמה הזכות לנהל מו"מ עם שתי ההצעות המיטביות.

1.8. בחירת הזוכה תעשה בדרך של שקלול המרכיבים המפורטים להלן, והכל על פי שיקול דעתה הבלעדי של מכבי ובאופן שתבחר ההצעה המעניקה למכבי את מירב היתרונות:

מחיר - 60%, איכות - 40%.

1.8.1. **ציון המחיר:**

ציון המחיר ייקבע על פי הצעת המחיר בסעיף 5.4 להלן. המציע בעל ההצעה הנמוכה ביותר יקבל את מלוא ציון המחיר, והמציעים האחרים יקבלו ציון מחיר יחסי ביחס אליו.

1.8.2. **ציון האיכות:**

יינתן עפ"י התרשמות מהתוצרים המבוקשים ועמידה בתנאים כמפורט בטבלה בסעיף 2.6 להלן.

1.9. הצעה זו אינה מבטלת את זכותה של מכבי להמשיך התקשרויות קודמות, בהתאם לשיקול דעתה הבלעדי, עם מציע, ואין בעובדה שמציע הציע את הצעתו במסגרת בקשה זו על מנת לבטל ו/או לשנות ו/או לגרוע מזכויות מכבי בהתאם להסכמים קודמים עימו, לרבות מימוש אופציות ככל שהן קיימות.

1.10. ספקים עימם תתקשר מכבי, יחתמו על ההסכם המצורף לבקשה תוך 7 ימים מקבלת הודעה על רצונה של מכבי להתקשר עימם. מסמכי הבקשה והצעת הספק יהוו חלק בלתי נפרד מהסכם ההתקשרות שייחתם.

1.11. ידוע למציע שמכבי תהא רשאית להציג את פרטי הצעתו הכלכלית, ככל שתוכרז כזוכה, בפני מציעים אחרים.

2. <u>תהליך בחינה של ההצעה:</u>

2.1. **עלות ההצעה** - מחיר כולל (FIX) עבור כל הדרישות המוגדרות בבקשה.

2.2. **הספק כחברה** - יכולת לספק את השירותים ואת צוות המומחים למתן השירותים הנדרשים המתוארים במסמך זה.

2.3. **ניסיון** - ניסיון של הספק במתן שירותים מקצועיים ושירותי תמיכה ללקוחות גדולים עם יותר מ- 1000 עמדות קצה, בפרט ניסיון בהתקנה, הטמעה ומתן שירותי תמיכה לגבי המוצר המוצע, כולל הוכחת ביצוע.

2.4. **איכות** – איכות הפתרון המוצע ואיכות שירותי הספק.

2.5. **בסעיף מגוון והמלצת לקוחות -** מכבי שומרת לעצמה את הזכות לפנות באופן עצמאי ועל פי שיקול דעתה לגורמים אשר מבצעים שימוש בשירות.

2.6. להלן פירוט המשקולות לבחינת ההצעות:

<u>עלות</u>	<u>60%</u>	
עלות המערכת בהתאם לדרישות הבל"מ	100%	
סה"כ עלות	**100%**	
<u>איכות</u>	<u>40%</u>	<u>ציון סף מינימלי</u>
הערכת הספק, יכולות הספק	10%	75%
ניסיון הספק והצוות בפרויקטים דומים	20%	75%
מגוון והמלצת לקוחות	30%	75%
איכות הפתרון והשירות המוצע	10%	75%
עמידה בדרישות והתאמה לצרכי מכבי	25%	75%
איכות המענה	5%	75%
סה"כ איכות	**100%**	75%

רמת סף מינימלית לציון עובר במדד האיכות: מצוינת לכל סעיף בנפרד ו- 75% בשקלול האיכות הכולל. ציון איכות הנמוך מרמת הסף, יפסול את הצעת המציע.

3. רקע

3.1. מכבי מעוניינת לרכוש מוצר תוכנה לצורך בקרה על מערכות אבטחת המידע והגנת הסייבר בארגון. המערכת תהווה פלטפורמה לביצוע התקפות, זיהוי חולשות וכשלים, גזירת משמעויות והוצאת המלצות לטיפול בכלל אזורי משטח התקיפה הארגוני במכבי.

3.2. על המערכת לאפשר מגוון גדול ועדכני של סימולציית התקפות אוטומטיות או מותאמות אישית ע"י צוות האנליסטים במכבי ובכל ערוצי הפעילות הקיימים בארגון כגון: מייל, גלישה, WAF, תחנות קצה, תנועות ברשת הארגון, חסינות DLP, כלי אבטחת המידע השונים בארגון ועוד.

4. המפרט המבוקש:

על המציע לציין בכל סעיף האם קיים/ לא קיים.

4.1. דרישות חובה

מספר	דרישה	מענה הספק
	דרישות כלליות	
1.1.	The solution must be deployable in a production on-premises/on-premises Private Cloud/Public cloud/Public-Private Hybrid Cloud environments.	
1.2.	For the proposed Solution, The Simulation agent should be compatible on Windows, Linux (All flavours including but not limited to Ubuntu, RHEL, Cent OS), MAC OS etc.	
1.3.	The solution must support proxy communications to the Internet. Simulation Agents installed must support proxy communications to the Breach & Attack simulation solution's cloud platform counterpart.	
1.4.	For the proposed solution, Agents will be installed on minimum set of endpoints. Considering mentioned setup supplier should be	

	able to run and provide all required use cases/simulations effectively	
	The solution must be easily and automatically updated either from the server itself or via manual updates	.1.5
	For the proposed Solution, All installed agents/simulators should have capability to run assessments/simulations as local user privilege and/or admin user privilege	.1.6
	For the proposed solution, If cloud based then all data collected/processed should be secure in vendors cloud instance.	.1.7
	The solution must directly integrate with common commercial SIEM solutions – including Qradar and Demisto	.1.8
	The solution must directly integrate with common commercial endpoint security controls including Mcafee and Microsoft ATP	.1.9
	The solution must validate network security control effectiveness.	.1.10
	The solution must include support for the POP3, IMAP, and SMTP email protocols with SSL and TLS.	.1.11
	The solution should have technical integrations available for specific vendors where applicable (e.g. SIEMs, ITSM's, ticketing systems, Vulnerability assessment tools, log management, Firewalls, SOAR, automation/orchestration, analytics platforms, threat intelligence platforms, etc.)	.1.12
	For the proposed solution, The Supplier shall describe/provide assurance that when the customer deletes data, the data is completely	.1.13

	gone and not resident anywhere on the supplier infrastructure within the solution.	
ניהול משתמשים והרשאות במערכת		
	For the proposed solution, The Supplier should ensure access to sensitive information is restricted to only personnel with a need to know basis with Granular User Role management	.1.14
	The solution must include discrete privileged and user account levels with specific permissions for each (e.g. RBAC)	.1.15
	The Solution should have Multi-Factor Authentication to access Platform And access list for any computer	.1.16
	The solution must include basic user policy controls for account access and password management	.1.17
	The proposed solution should respond with a generic error message regardless of whether the user ID or password was incorrect. The message should give no indication of the status of an existing account	.1.18
	The solution must generate an audit log of all operations including individual user actions	.1.19
	The Supplier should ensure passwords for services shall not be displayed during authentication nor stored in an unencrypted form	.1.20
	The Supplier proposed solution should secure audit logs from tampering.	.1.21
Use Cases		
	Solution should have Ability to simulate breach methods across the complete cyber-attack kill chain including NIST, MITRE att&ck complete framework (e.g., infiltration, exfiltration etc)	.1.22
	The solution should include attacks simulations relevant to information technology targets, FinTech Targets, BFSI Targets, NBFC Targets	.1.23
	The solution must include library of attacks that exploit common application vulnerabilities & Weaponize Known CVE's.The solution must be able to Represent Vulnerability Risk scores (Low, Medium, High, Critical) based on proven cybersecurity risk assessment models. (e.g. DREAD, CVSSV3, NIST)	.1.24

	Solution must provide time-stamp of the attack across multiple geographies for all attack vectors for correlation & Validation.	.1.25
	Solution should have Ability to test data loss prevention (DLP) implementation, methodology, and configuration along with other exfiltration techniques to test outbound flows of data to ensure protection of critical information	.1.26
	Solution should have Ability to simulate Infiltration techniques for breaching a network or infecting a host - Via Email, Web & WAF.	.1.27
	Solution should have Ability to simulate Machine-based attacks - known vulnerabilities on internet-facing systems, misconfiguration of network perimeter controls, exposed applications, etc	.1.28
	Solution should have ability to conduct the complete full kill chain of the attack. That is end to end attack execution from pre exploitation stage to exploitation to post exploitation.	.1.29
	Solution should have Ability to test attacker lateral movement through a single machine (once successfully within a network) - e.g., brute force or pass-thehash techniques to steal credentials for sensitive servers, moving across network segments in search for valuable data	.1.30
	Solution should support Ransomware simulations	.1.31
	Solution should support Email security assessment (improper configuration or implementation of email filters)	.1.32
	Solution should support Endpoint Assessment - test security state of endpoints by comprehensively testing: automated behavioral detection (EDR), signature-based detection (anti-virus), known vulnerabilities including Windows patches.	.1.33
	Solution should support Extracting credentials from memory (Endpoint privilege escalation test)	.1.34
	Solution should support Executing local privilege elevation exploits (Endpoint privilege escalation test	.1.35
	Solution should support Transfer and/or execution of malware on a test system (Endpoint malware download and execution test)	.1.36

	Solution should support Access, connection, or data transfer attempt (Network segmentation test)	.1.37
	Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test) on cloud drives (e.g. Gdrive, onedrive, dropbox, slack etc.)	.1.38
	Solution should support Access or data transfer to a malicious site (Secure web gateway / proxy test)	.1.39
	Solution should support Proxy tests - HTTP/HTTPS inbound/outbound exposure to malicious or compromised websites (web malware, malicious scripts)	.1.40
	Solution should have Ability to deliver safe tests with no chances of interfering with business operations, and no user interference when deployed on production assets	.1.41
	Solution should have Ability to simulate breach methods based on attacker profile (APT) and data assets to be protected	.1.42
	Solution should have Mechanism to identify remediation options and recommendations, prioritize severity of test findings and actionable remediation for each security control.	.1.43
	The Solution should provide POA (Proof of acceptance) for manual assessments / simulation along with Mitigation steps.	.1.44
	Solution should Continuously simulate breach methods to address changing risks, and track security posture via risk trending and historical reports.	.1.45
	Solution should have Test Security Operations Centre (SOC)rules by simulating a multi-vector attack	.1.46
	Solution should have Ability to create custom use cases / simulations attacks according to client requirement	.1.47
	Solution should Test effectiveness of security controls (real behaviour and outcome of controls) - e.g., identify configuration errors or defect	.1.48
	The solution should provide technology vendor-specific remediation signatures and prioritization as mitigation recommendations	.1.49

	The Supplier proposed solution should have capabilities to allow for the detection or prevention of unauthorized modification of data.	.1.50
	The Supplier should validate and measure the detection and response capabilities of security pipelines and detection analysts in the SOC	.1.51
	The Supplier should verify SIEM alerts by simulating malicious activity (injecting events into a SIEM) to gauge whether it correlates them to generate the right alert (Monitoring SIEM tests)	.1.52
	The Supplier should address configuration, segmentation or implementation errors throughout the entire lifecycle of a security product	.1.53
	The Supplier should address configuration, segmentation or implementation errors throughout the entire lifecycle of a security product	.1.54
	The solution should supports Azure & AWS cloud endpoints.	.1.55
	The solution should support use cases specific to Kubernetes, Docker, Container deployments	.1.56
Dashboards דוחות		
	The solution must include graphical dashboards of the results of security effectiveness validation	.1.57
	The solution must include at least one graphical dashboard that provides quantitative results by numeric count and by percentage of attacks by stage	.1.58
	The solution dashboard must include summary reporting and visual graphs of the results of executed attacks	.1.59
	The solution must include the ability to export primary dashboards, reporting in PDF format	.1.60

4.2. **<u>דרישות חומרה ותוכנה</u>**

4.2.1. המערכת המבוקשת תותקן בתצורת ענן.

4.2.2. יש לפרט את רכיבי התשתית, חומרה ותוכנות מדף נדרשים, כולל גרסאות, על מנת לממש את המערכת. הצטיידות רכיבי התשתיות הנדרשות תתבצע על ידי מכבי, מחוץ לתכולת הצעת הספק.

4.3. **<u>דרישות תחזוקה ותמיכה</u>**

4.3.1. תמיכה על ידי הספק במערכת, לתקופת תחזוקה הכלולה בהצעה זו מיום האספקה בפועל.

4.3.2. קבלת עדכונים ושדרוגי גרסאות שוטפות, תיקוני באגים , Hotfixes , Patches וכד׳.

4.3.3. יכולת של מכבי לפתיחת תקלות, אירועים וקבלת תמיכה של היצרן, לפי המפורט בסעיף SLA.

4.3.4. תמיכה ותחזוקה של המערכת תבוצע ממשרדי מכבי בלבד אלא אם מכבי תאשר לספק להתחבר מרחוק.

4.4. **<u>זמן תגובה נדרש (SLA) מהספק</u>**

4.4.1. לתקלות רגילות - תמיכה טלפונית לפי שעות עבודה בזמן ישראל, NBD.

4.4.2. במידה והבעיה לא נפתרת תהיה אפשרות לנציג מכבי להעלות את רמת החומרה.

4.4.3. לתקלה משביתה נדרש זמן תגובה של עד 5 שעות בשעות הפעילות ועבודה רציפה על תיקון התקלה.

4.5. **<u>דרישות מספק הפתרון</u>**

4.5.1. באם הצעת הספק כוללת מוצרי צד ג׳, על הספק להיות מורשה מטעם היצרן למכירת המוצרים המוצעים.

4.5.2. על הספק להיות בעל הסמכה של יצרן המוצרים המוצעים להתקנה, הטמעה ותחזוקה של המערכות המוצעות.

4.5.3.על הספק להוכיח קיום קשרי עבודה עם יצרן המערכת המוצעת (פתיחת תקלות, יכולת שינויים ,עדכונים וכדומה).

4.5.4.רשימת לקוחות וממליצים רלוונטיים אשר הטמיעו את המוצר בסביבות עבודה מורכבות. לכל לקוח נדרש לציין את הרלוונטיות שלו לבקשה זו, תיאור הפתרון, שמות אנשי קשר וטלפונים לקבלת מידע נדרש.

4.5.5.יש לציין את כוח האדם המוצע לפרויקט זה ולפרט את ניסיונו בהתקנה ואינטגרציה של המוצר בישראל.

4.5.6.על הספק לסיים את התקנת המערכת בתוך פרק זמן של חודש מסיום התקנת התשתיות הנדרשות ע"י מכבי, כולל פיתוחים, התאמות ובדיקות.

5. <u>טופס ההצעה (מהווה את נספח א' להסכם):</u>

5.1. שם הספק המציע: _____

5.2. פירוט המלצות ולקוחות קיימים למערכת (כתובת המייל מדומיין הלקוח בלבד) – יש להעביר 2 המלצות לפחות עבור המערכת והטמעתה בחברה הממוקמת בישראל – על הממליץ להיות לקוח קצה אשר מנהל את המערכת בפועל ולא חברת ייעוץ / נותנת שירותים באמצעות המערכת ללקוחות:

שם חברה	שנות וותק בשירות	איש קשר	תפקיד	טלפון	מייל

5.3. **<u>על הצעת המחיר לכלול:</u>**

5.3.1. הטמעת

5.3.2. הכשרה לפחות של 2 מנהלי מערכת במכבי ע"י הספק לאחר הטמעת הפתרון, בין אם על ידי קורס או ימי הכשרה באתר הלקוח.

5.3.3. תמיכה שוטפת בתקלות11.

5.4. **<u>טופס הצעת המחיר:</u>**

	עלות FIX	הערות
עלות מערכת המותאמת למכבי בהתאם לדרישות המפורטות בהצעה, **<u>כולל</u>**: • רישוי • התקנה בסיסית • הטמעה • הדרכה • אחריות ותחזוקה **לשנה אחת**		

- המחירים אינם כוללים מע"מ
- המחירים יהיו נקובים בשקלים.

- תנאי תשלום- שוטף +65 מיום הוצאת החשבונית.
- התשלום יתבצע מידי חודש, בהתאם לשעות העבודה בפועל שבוצעו, בהסתמך על דו"ח ריכוז שעות עבודה אשר יועברו למכבי ע"י הספק
- תוקף ההצעה- 90 ימים.

תאריך : _____

<u>הסכם</u>

מיועד עבור הספק/ים הזוכה/ים בלבד. אין צורך למלא ולחתום בשלב הגשת ההצעה!!!

בין מכבי שרותי בריאות (**להלן: "מכבי"**) לבין _____ח.פ._____ (להלן: "**הספק**").

לאספקת: **<u>מערכת בקרה למערכות אבטחת מידע (BAS) במכבי והשירותים הנלווים למערכת</u>**
(להלן: "**המוצרים והשירותים**")

1. <u>תקופת ההסכם</u>

1.1 הסכם זה יעמוד בתוקף למשך **<u>שנה</u>** החל מיום _____ ועד יום _____ (**להלן: "תקופת ההסכם**").

1.2 על אף האמור לעיל בסעיפים 1.1 ו – 1.2, מכבי תהא רשאית להביא הסכם זה לידי סיום, בכל שלב ומכל סיבה שהיא, וזאת על-ידי משלוח הודעה בכתב 60 יום מראש. במקרה זה תשלם מכבי לספק את הסכומים שהתחייבה לשלם עד למועד שבו הופסקה ההתקשרות, או הספק יחזיר למכבי את הסכומים ששולמו עבור התקופה שלאחר מועד הפסקת ההתקשרות.

2. <u>תמורה</u>

2.1 רשימת השירותים המסופקים על ידי הספק למכבי ומחיריו יהיו כמפורט במחירונים המצ"ב **<u>כנספח א'</u>** להסכם זה.

2.2 היה והספק יזכה בבקשה של החשב הכללי לאספקת נשוא ההסכם במהלך תקופת ההתקשרות עם מכבי, תעמוד למכבי הזכות, על פי שיקול דעתה הבלעדי, להתקשר עם הספק הזוכה על בסיס המחירים בהם זכה בחשב הכללי, מתחילת התקשרותו עם החשב הכללי ועד סיום ההתקשרות עם החשב הכללי.

3. <u>תנאי תשלום</u>

3.1 התמורה תשולם כנגד חשבונית מס בתנאי תשלום של שוטף + 65 יום ממועד הפקת החשבונית. החשבונית תוגש לא יאוחר מ- 10 (עשרה) ימים מתום חודש הפעילות. אם תוגש לאחר מועד זה, התשלום ידחה למועד התשלום הבא.

3.2 הספק יציג בפני מכבי אישור עפ"י חוק עסקאות גופים ציבוריים (אכיפת ניהול חשבונות) תשל"ו – 1976 המעיד על ניהול פנקסי חשבונות עפ"י פקודת מס הכנסה וחוק מע"מ או פטור מניהול זה, על כי הוא נוהג לדווח לפקיד השומה על הכנסותיו וכן נוהג לדווח על עסקאותיו למע"מ בהתאם לחוק.

4. <u>זכויות קנין רוחני</u>

4.1 הספק מצהיר כי הוא בעל הזכויות בשירות וכי אין כל מניעה חוקית או אחרת המונעת ממנו לספק בכל דרך את הציוד למכבי וכי אין באספקת הציוד משום הפרת פטנט ו/או פגיעה כלשהי בזכויות של חברה ו/או גוף לרבות אדם אחר כלשהו.

4.2 היה ותתבע מכבי על-ידי גורם כלשהו בגין הפרת זכויות וטענות של צד שלישי בציוד, מתחייב הספק לשפות לאלתר את מכבי בגין כל הוצאה שתיגרם לה כתוצאה מתביעה שכזו.

5. <u>מועסקי הספק</u>

5.1 הספק מצהיר בזה, כי כל האנשים שיועסקו על ידו לצורך אספקת השירות למכבי ייחשבו לכל צורך כעובדיו או שלוחיו ולא יחשבו כעובדיה או שלוחיה של מכבי, במישרין או בעקיפין, ויועסקו על ידו באופן בלעדי, על חשבונו הוא בלבד, ועליו תחול האחריות לגבי תביעותיהם הנובעות מיחסיו עימם.

5.2 הספק יהא אחראי כלפי עובדיו, שליחיו וכל מי שפועל מטעמו בגין מוות, נזק גופני, או נזק לרכוש שייגרם להם, בין במישרין ובין בעקיפין, כתוצאה מתאונה או מנזק שאירע בעת אספקת השירות.

5.3 הספק מתחייב לפצות ו/או לשפות את מכבי, בגין כל נזק ו/או הוצאה שיגרמו לה, אם יקבע על ידי רשות מוסמכת, כי המצב המשפטי ו/או העובדתי שונים מהמוצהר בהוראות פרק זה.

5.4 הספק מתחייב שכל נותן שירות מטעמו למכבי חייב להיות מחוסן עפ"י תוכנית החיסונים המוגדרת ע"י משרד הבריאות.

6. <u>אנשי קשר</u>

6.1 מכבי ממנה בזאת את **אבישי ויספיש** להיות איש הקשר הישיר עם הספק.

6.2 הספק ממנה בזאת את _____ להיות איש הקשר הישיר עם מכבי.

שם: _____ טלפון: _____

סלולרי: _____ EMAIL: _____

7. <u>הסבת הסכם</u>

הספק איננו רשאי למסור, או להעביר לאחר, את זכויותיו על פי ההסכם, או את החובות הנובעות ממנו, אלא בכפוף לאישור מראש ובכתב של מכבי.

8. <u>אחריות וביטוח</u>

8.1 הספק יהא אחראי לנזק ו/או אובדן מכל סוג שהוא, לרבות נזק שיגרום הוא ו/או מי מטעמו, לגופו ו/או לרכושו ו/או לעסקו של כל אדם ו/או גוף, לרבות, למכבי ו/או למי מטעמה ו/או לצד שלישי כלשהו, שנגרם תוך כדי ו/או בקשר עם מתן השירותים ו/או הסכם זה.

8.2 הספק מתחייב לפצות ו/או לשפות את מכבי, מיד עם דרישתה הראשונה, בגין כל נזק ו/או הוצאה שייגרמו למכבי, לרבות הוצאות ושכ"ט עו"ד בגין תביעה ו/או דרישה שתוגש נגד מכבי, כתוצאה ו/או בקשר עם אחריות הספק ו/או מי מטעמו, על פי הסכם זה ו/או על פי כל דין, וזאת מבלי לגרוע מזכויות מכבי לכל תרופה או סעד על פי הסכם זה ו/או על פי כל דין ובלבד שנמסרה הודעה לספק וניתנה לספק הזדמנות להתגונן בפני כל דרישה ו/או הוצאה ו/או תביעה כאמור.

8.3 מבלי לגרוע מאחריות ומהתחייבות הספק על-פי הסכם זה ו/או על-פי כל דין, ממועד תחילת הסכם זה או ממועד תחילת מתן השירותים, לפי המוקדם ,הספק מתחייב לערוך ולקיים ביטוחים הולמים, ככל שנהוגים בתחום פעילותו: ביטוח חבות מעבידים, ביטוח אחריות כלפי צד שלישי, ביטוח אחריות מקצועית, בגבולות אחריות סבירים בהתאם לאופיים והיקפם של השירותים המבוצעים על ידו וזאת למשך כל תקופה ההסכם לרבות כל הארכה שלו.

8.4 ככל שיועסקו על ידי הספק קבלני משנה, עליו לדרוש כי הללו יערכו ביטוחים בהתאם לאופי והיקף ההתקשרות, או לחילופין לכלול בביטוחיו כיסוי לפעילותם.

8.5 הספק יוודא כי בכל ביטוחיו המתייחסים לשירותים נשוא ההתקשרות תיכלל הרחבת שיפוי כלפי מכבי שירותי בריאות בגין אחריותם למעשי ו/או מחדלי הספק.

8.6 בהקשר זה מובהר, כי אין בעריכת הביטוחים הנ"ל על-ידי הספק כדי לצמצם או לגרוע בצורה כל שהיא מהתחייבויותיו בהתאם להסכם, ולא יהיה בעריכת הביטוחים כדי לשחרר את הספק מחובתו לשפות ו/או לפצות את מכבי שירותי בריאות ו/או מי מטעמה בגין כל נזק שהספק אחראי לו על-פי הסכם זה ו/או על-פי כל דין.

8.7 הביטוחים יכללו תנאי מפורש, על פיו הינם קודמים לכל ביטוח אשר נערך על-ידי מכבי שירותי בריאות, וכי המבטח מוותר על כל דרישה או טענה בדבר שיתוף ביטוחי מכבי שירותי בריאות. כמו כן, יתחייב המבטח שהפוליסות לא תצומצמנה ולא תבוטלנה, אלא אם תימסר הודעה בכתב בדואר רשום לידי מכבי לפחות 30(שלושים) יום מראש

8.8 הספק יוודא כי בכל ביטוחיו המתייחסים לשירותים נשוא ההתקשרות ייכלל סעיף ויתור על זכות התחלוף/השיבוב כלפי מכבי שירותי בריאות עובדיה והפועלים מטעמה (ויתור כאמור לא יחול בגין נזק בזדון).

8.9 מכבי שומרת לעצמה את הזכות לקבל מהספק אישור על קיום ביטוח או העתקי פוליסות, לפי דרישה.

8.10 מוסכם בזאת במפורש, כי נוסחי פוליסות הספק, למעט ביטוח אחריות מקצועית, לא יהיו נחותים מהנוסח הידוע כ"ביטי" הרלוונטי למועד עריכת הביטוח או כל נוסח אחר שיחליף אותם.

8.11 אי עמידה בתנאי סעיף זה מהווה הפרה של הסכם זה.

9. <u>פרסום, שמירת סודיות ואבטחת מידע</u>

9.1 הספק מתחייב לשמור בסוד, ולא להעביר, למסור ו/או להביא לידיעת כל אדם, כל ידיעה בקשר עם ביצוע ההסכם או השירות או ידיעה שהגיעה אליו בתוקף או במהלך או אגב ביצוע ההסכם או מתן השירות, תוך תקופת ההתקשרות, לפני תחילתה או לאחר סיומה.

9.2 הספק מצהיר, כי ידוע לו שהפרת ההתחייבות האמורה מהווה עבירה לפי סעיף 118 לחוק העונשין, התשל"ז-1977.

9.3 כל פרסום בקשר להסכם זה ו/או שימוש בשמה של מכבי, לרבות בסימני המסחר שלה, כפופים לקבלת אישורה מראש ובכתב של מכבי.

9.4 **דרישות לסודיות:**

הספק מצהיר ומתחייב כדלקמן:

9.4.1 לשמור על סודיות מוחלטת ביחס לכל המידע שנכלל במסמכי ההסכם וכן ביחס לכל מידע על ושל מכבי, עובדיה, מבוטחיה, שיטות עבודתה, נתוניה הכספיים, מידע על ספקיה, מידע רפואי, מידע ניהולי, מידע עסקי, מידע פיננסי וכיו"ב נתונים, אשר יגיעו לידיעתו במסגרת ביצוע התחייבויות הספק על-פי האמור במסמכי הסכם זה (להלן: "המידע").

9.4.2 למנוע כל פרסום ו/או גילוי של המידע בכל דרך שהיא ובכל זמן שהוא, אלא אם קיבל אישור ספציפי, לכל נושא בנפרד, בכתב, מאת מכבי ובהתאם לאישור שניתן.

9.4.3 לעשות את כל הסידורים הדרושים לשמירת המידע, להגביל את הגישה למידע אך ורק לעובדי הספק המורשים לכך, ולדאוג לכך שכל עובדי הספק, נותני שירותים והמועסקים על ידו ומטעמו לצורך ביצוע התחייבויותיו על-פי ההסכם יחתמו על כתב התחייבות אישי לשמירת סודיות כלפי הספק (בכל עת), בנוסח המחייב אותם לעמוד בהתחייבויות הספק לשמירת סודיות המפורטות בהסכם זה, וכן כלפי מכבי (בהתאם לדרישה מפורשת ולנוסח שיומצא על-ידי מכבי).
מובהר בזאת, למען הסר ספק, כי הספק יהא אחראי כלפי מכבי למילוי האמור על-ידי עובדיו ו/או הפועלים מטעמו או עבורו.

9.4.4 חובת שמירת הסודיות המפורטת לעיל לא תחול על:

9.4.4.1 מידע שהיה בידי הספק ו/או בידי עובדיו ו/או נותני השירות מטעמו טרם ההתקשרות בהסכם זה שלא עקב הפרת התחייבות לשמירת סודיות;

9.4.4.2 מידע שנתקבל מצד ג' באופן עצמאי שלא עקב הפרת התחייבות לשמירת סודיות;

9.4.4.3 מידע שהוא או הפך נחלת הכלל שלא בגין הפרת התחייבות לסודיות של הספק.

9.4.4.4 מידע שחובה לגלותו על-פי דין או על-פי צו מרשות שיפוטית מוסמכת, ובלבד שהספק הודיע למכבי ללא דיחוי אודות צו כאמור, ואפשר לה להתגונן מפניו.

9.4.5 כי ידוע לו והוא מסכים שכל המידע הוא בבעלותה הבלעדית של מכבי, וכי הספק לא יהא רשאי לעשות בו כל שימוש שאינו לצורך ביצוע ההסכם.

9.4.6 כי ידוע לו שייתכן והוא ייחשף גם למידע רגיש ביותר, לרבות מידע אשר קיימת לגביו התחייבות מפורשת או משתמעת של מכבי כלפי צדדים שלישיים לשמור עליו בסודיות, ואשר גילויו לאחרים או שימוש בו שלא לצורך ביצוע ההסכם עלול לגרום למכבי נזקים והפסדים ולהפרת התחייבות לשמירת המידע בסודיות, וכי הספק מודע לכך שהמידע הינו חלק מנכסיה של מכבי.

9.4.7 כי ידועות לו הוראות הדין הקובעות את חובת שמירת הסודיות, והוא מודע לסנקציות האזרחיות והפליליות (בנוסף לצעדים בגין הפרת ההסכם) להן הוא צפוי אם הוא או מי מעובדיו מי מטעמו יפר הוראות אלו, לרבות (אך לא רק) הוראות חוק הגנת הפרטיות, התשמ"א-1981 ותקנותיו, חוק זכויות החולה, התשנ"ו-1996, וכל דין רלבנטי נוסף.

9.5 **דרישות אבטחת מידע:**

הספק מצהיר ומתחייב כדלקמן:

9.5.1 כללי

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

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

9.5.1.3 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.

9.5.1.4 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.

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

9.5.1.6 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.

9.5.1.7 יש לדווח למנהל אבטחת המידע והגנת הסייבר במכבי בכל חשד לאירוע אבטחת מידע בעל השפעה על המידע של מכבי.

9.5.1.8 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.

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

9.5.1.10 הספק ועובדיו לא הורשעו בעבירה שיש עמה קלון ו/או עבירה שנושאה כספי (כגון אי העברת ניכויים ואי דיווח לרשויות המס), זולת אם חלפה תקופת ההתיישנות לפי חוק המרשם הפלילי ותקנות השבים, התשמ"א- 1981 ו/או במועד הגשת ההצעות בהליך זה, לא מתנהלים

נגדו הליך משפטי ו/או חקירה בעבירות כאמור לעיל; אם המציע הוא תאגיד-נדרש כי העדר הרשעה וחקירה כאמור יתקיים גם לגבי בעל השליטה בו ונושאי המשרה שלו.

9.5.2 אבטחה לוגית במערכת

9.5.2.1 הספק יישם מידור פנימי במערכת. הגישה תתאפשר רק למי שעבודתם ותפקידם אצל הספק מחייבים זאת, ולמי שחתמו על התחייבות לשמירת סודיות מול מכבי.

9.5.2.2 במערכת תשמר אבטחת המידע באופן הבא:

9.5.2.2.1 הכניסה למערכת תהיה באמצעות USER ID וסיסמא אישית .

9.5.2.2.2 אורך הסיסמא יהיה לפחות שבעה תווים.

9.5.2.2.3 הסיסמאות יוחלפו כל שלושה חודשים לפחות.

9.5.2.2.4 התחנה תינעל אוטומטית לאחר 5 שגיאות רצופות בהקשת הסיסמא.

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

9.5.2.2.6 תותקן תכנת הגנה תקנית ומעודכנת כנגד וירוסים.

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

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

9.5.2.4 גישה מרוחקת למערכת תבוצע לכל הפחות על בסיס הגדרות האבטחה הבאות:

9.5.2.4.1 יבוצע "זיהוי חזק" כפול בעת הגישה לשירות.

9.5.2.4.2 יוגדר לוג אירועים על השימוש בשירות.

9.5.3 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 הבאים, מכל אתר ומכל מחשב ממנו יתחבר לרשת מכבי:

9.5.3.1 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.

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

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

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

9.5.3.5 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

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

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

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

9.5.4 ניטור ובקרה

9.5.4.1 יוגדר ויופעל לוג אירועים מלא במערכת.

9.5.4.2 לוג אירועים יופעל על האירועים הבאים:

9.5.4.2.1 כניסות למערכת – מוצלחות או כישלונות.

9.5.4.2.2 כל גישה לנתונים, כולל קריאה בלבד.

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

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

9.5.4.2.5 שינוי הגדרות מערכת. כולל שינוי במערכת המשתמשים וההרשאות.

9.5.4.3 רישום כל אירוע יכלול את הערכים הבאים:

9.5.4.3.1 מועד ביצוע הפעולה.

9.5.4.3.2 שם משתמש מבצע הפעולה.

9.5.4.3.3 כתובת מקור.

9.5.4.3.4 סוג ה – Client.

9.5.4.3.5 שם הפעולה.

9.5.4.3.6 סטטוס – הצלחה\כישלון.

9.5.4.3.7 תיאור הפעולה.

9.5.5 אבטחת מידע בענן:

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

9.5.5.1 ספק הענן יהיה ב- EU Region בלבד

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

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

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

9.5.5.5 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.

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

9.5.5.7 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.

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

9.5.5.9 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, PCIחוק הגנת הפרטיות.

9.5.5.10 **ניהול זהויות והרשאות בענן:**

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

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

9.5.5.11 **אחסון מידע**

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

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

9.5.5.12 **הצפנת המידע**

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

9.5.5.12.2 ההצפנה תבוצע בהתאם לסטנדרטים המקובלים בשוק.

9.5.5.12.3 מפתחות ההצפנה יישמרו באופן בלעדי בידי הארגון במידת האפשר.

9.5.5.13 **ניטור אירועים** – יוגדר ויופעל לוג אירועים על פי סעיף 9.5.4

סעיף זה, על כל סעיפי המשנה לו, הינו סעיף עיקרי בהסכם, אשר הפרתו מהווה הפרה יסודית של ההסכם.

10. <u>שונות</u>

10.1 הצדדים להסכם מסכימים בזה, כי למכבי, <u>ולה בלבד</u>, תהיה זכות לקזז כל חיוב כספי שהספק עשוי להיות חב לה מתוך העסקה נשוא ההסכם או מעסקה אחרת, מכל סכום שיגיע לספק ממכבי.

10.2 הספק מצהיר בזה, כי הוא מסכים לכך שההרשאה שניתנה לו על ידי מכבי לספק את השרות אינה בלעדית.

10.3 לכל התאגידים / חברות בקבוצת מכבי, לרבות, אך לא רק: אסותא מרכזיים רפואיים בע"מ, בית בלב בע"מ, מכבידנט בע"מ, עמותת קרן מכבי ומכבי טבעי, מכבי-קאר בע"מ, מכבי אחזקות בע"מ, אגודת מכבי מגן, מכבי יזמות וכד' תהא שמורה הזכות לרכוש את המוצרים מהספק על פי המחירים, ושאר תנאי ההסכם הקבועים בהסכם זה.

10.4 לדרישת מכבי, הספק יערך תוך שלושה חודשים לעבודה במתכונת של חשבונית מרכזת, בליווי קובץ ממוחשב, במבנה שתגדיר מכבי.

10.5 כתובות הצדדים הן כמפורט להלן. כל הודעה בקשר להסכם זה שתשלח בדואר רשום על ידי צד למשנהו על פי הכתובת כמפורט לעיל, תחשב כאילו התקבלה על ידי הצד אליו נשלחה תוך 3 ימים מיום המשלוח, ובמקרה בו נמסרה ביד - בעת המסירה בפועל.

מכבי שירותי בריאות – רח' המרד 27 תל אביב, 68125

הספק _____ רח' _____

כתובות הדואר האלקטרוני של הצדדים:

מכבי: _____

הספק: _____

ולראיה באו הצדדים על החתום :

_____	_____
מכבי שרותי בריאות	הספק

שם מלא של החותם: _____ חותמת: _____

<u>אישור</u>

אני הח"מ, _____, עו"ד, מאשר כי מר/גב' _____, נושא/ת ת.ז. מס' _____, ומר/גב' _____, נושא/ת ת.ז. מס' _____, הינו/ם מוסמכים לחתום על הסכם זה מטעמה של _____, ח.פ./שותפות/עמותה רשומה מס' _____, וכי חתימתו/ם, בצרוף חותמת התאגיד הנ"ל, מחייבת ומזכה את התאגיד הנ"ל לכל דבר ועניין.

_____

_____, עו"ד