מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

נספח ג' מכרז 10003350
דרישות מחשוב והגנת הסייבר לאפליקציות

מספר מכרז: _____ תאריך: _____

מהות האפליקציה: _____

שם הספק: _____

שם רפרנט המערכת : _____ סלולרי: _____

מייל הרפרנט: _____@_____

שם ממונה אבטחת המידע : _____ סלולרי: _____

מייל ממונה אבטחת מידע: _____@_____

דרישות סף:

- סעיפים עם כוכבית (*) – סעיף שלא יסומן כמקובל לא יעמוד בדרישות הסף
- מערכות הפעלה ומערכות הגנה הנמצאות **בתמיכת יצרן**
- מערכות הפעלה המקבלות עדכוני אבטחה באופן שוטף בהתאם למדיניות הארגון
- עדכוני אבטחה שסווגו כקריטיים על ידי היצרנים השונים יתבצעו במידי לפי הנחיית צוות אבטחת מידע וסייבר של המרכז הרפואי שיבא תל-השומר

בנוסף למענה, יש לצרף את המסמכים הבאים:

1. מסמך ארכיטקטורה מפורט של המערכת הכולל את פרוטוקולי התקשורת אתם היא עובדת, ממשקים למערכות, קלטים ופלטים.
2. תקני אבטחת מידע שהחברה מוסמכת אליהם.
3. מסמך מדיניות פיתוח מאובטח (SSDLC)
4. דו״ח מבדק חדירה ו/או סקר סיכונים אחרון שבוצע ב 18 חודשים האחרונים.
אם לא ניתן לצרף את הדו"ח המלא, נא לצרף דו"ח נקי הכולל את רמת הסיכון של המערכת, תאריך ביצוע הבדיקה, מבצע הבדיקה (שם) וחתימה.
5. נהלי גיבוי ו DR.

שם ממלא הטופס: _____ חתימה: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר ,מיקוד 5265601 , ישראל

1. <u>דרישות בנושא תשתית וארכיטקטורה.</u>

מחשב - לרשת בית החולים | Stand Alone | למחשב ייעודי (יש להקיץ בעיגול את המענה) | ענן שיבא | ענן חיצוני

- יש לציין את גרסת מערכת ההפעלה: _____
- סוג מערכת הפעלה כגון: (Pro/STD): _____
- יש לציין איזה Service Pack מותקן: _____

שרת - לרשת בית החולים | Stand Alone | למחשב ייעודי (יש להקיץ בעיגול את המענה) | ענן שיבא | ענן חיצוני

- יש לציין את גרסת מערכת ההפעלה: _____
- סוג מערכת הפעלה כגון: (Pro/STD): _____
- יש לציין איזה Service Pack מותקן: _____
- נא לציין גרסת OPENSSLבמידה ומותקן: _____
- נא לציין גרסת IIS/Apache במידה ומותקן: _____

סעיף	דרישה	מקובל/לא מקובל
1.1*	המערכת תיישם הפרדה בין שכבת היישום, האפליקציה , לשכבת הנתונים (חלק מנוהל פיתוח מערכות מאובטחות)	
1.2	שרתי בסיסי הנתונים ושרתי ה WEB/ אפליקציה יהיו נפרדים ולא באותו וילן	
1.3	שרת/מחשב צריך להיות בדומיין שיבא	
1.4	במידה והמערכת תותקן בענן שלא בבעלות שיבא, נדרש להגדיר חסימות על פי מיקום גיאוגרפי בהתאם לדרישות שיבא	
1.5	השרת יותקן וירטואלית תחת VMWARE ESX	
1.6*	מכשיר/מחשב/שרת שיסופק, יותקן עליו XDR הקיים בארגון ע"י נציגי בית החולים. מערכת הגנה XDR למערכות הפעלה Windows, Linux, Unix, MAC OS עדכונים של המערכת יבוצעו באופן שוטף על ידי הארגון יש לציין החרגות במידת הצורך _____ הספק יקשיח את רכיבי תשתיות המערכת (תקשורת, מערכות הפעלה, בסיסי נתונים וכדומה) על פי CIS best practice הרלוונטיים, כך שיתאפשר מתן השירות הנדרש בלבד	
1.7*	במידה וסעיף 1.6 סומן כ "לא מקובל" על היצרן להתקין תוכנת Application Control (**White List**) שתאושר ע"י צוות אבחת מידע והגנת הסייבר, המאשרת הפעלת קבצים לפי HASH או לפי Certificate והגנה מלאה על כל הכוננים במכשיר. **<u>יש לציין את הפרטים הבאים:</u>** שם המערכת: _____ גרסה: _____ • ההגנה תוגדר על כל הכוננים הקיימים הכולל חסימה על Disk on key • המוצר ייבדק ע"י נציג צוות הגנת הסייבר (שיבא) ונציג הספק/יצרן. יש לספק מהיצרן סיסמה למערכת ורשימת הקבצים המוחרגת.	
1.8	אם מופעל Firewall מקומי? האם ניתן לבטלו? (הקיפו בעיגול את התשובה)	כן / לא
1.9	במידה ולא ניתן לבטל Firewall מקומי. יש לבצע כללים (Rules) ב Firewall על פי הנחיית גורם אבטחת מידע בשיבא בזמן הטמעת המוצר.	

שם ממלא הטופס: _____ חתימה: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר ,מיקוד , 5265601 ישראל

1.10	במידה והמערכת עובדת מול בסיס נתונים, על הספק לתמוך ב SQL 2019 ומעלה	
1.11	הפרדת סביבות עבודה: סביבת הייצור תהיה מופרדת מהסביבות הנמוכות: בדיקות ופיתוח, וימוקמו בין השאר על גבי שרתים נפרדים. בנוסף, הסביבות הנמוכות לא יכילו מידע שיוגדר כחסוי	
1.12	מערכת הפעלה תותקן במרכז הרפואי ע"י צוות התשתיות (בשיתוף עם הספק)	
1.13	עדכוני אבטחת מידע בשרתי המערכת יתבצעו על ידי ביה״ח באופן סדור כאשר עדכונים שסווגו כקריטיים על ידי היצרנים השונים מתבצעים בסמוך להפצת העדכון.	
1.14	הקשחות השרתים ורכיבי המערכת יתבצעו בהתאם להנחיות אבטחת המידע של ביה״ח ובהתאם ל best practice של היצרנים	
1.15	במידה ויידרש מערך אחסון גדול לארכיון השטח יסופק בתצורת NAS , חובה תמיכה בפרוטוקול CIFS **יש לציין את הפרטים הבאים:** 1. גודל השטח שבועי: _____ GB 2. גודל שטח חודשי: _____ GB 3. גודל שטח שנתי: _____ GB	
1.16	תמיכה בעבודה מול האחסון ב Multi Share	

2. <u>דרישות בנושא אפליקציה והרשאות</u>

נא להקיף בעיגול:

- **שומר נתוני מטופלים** - בענן | מקומית בלבד | באחסון מרכזי | במערכת קלינית | אינו שומר
- **בשימוש** – משקי | מעבדתי | טיפולי/דיאגנוסטי | להתנסות זמנית

סעיף	דרישה	מקובל/לא מקובל
***2.1**	הפיתוח יתבצע על פי סטנדרט פיתוח מאובטח כגון תקן OWASP , STAR (CSA) והמערכת תעבור מבדקי חדירה אבטחתיים לבחינת האבטחה של הקוד הכוללים מבדקי DYNAMIC CODE	
***2.2**	המערכת תכלול מנגנון זיהוי ואימות המשתמש בחיבור ל Entra ID / AD (LDAPS), ולא תאפשר כניסה למערכת ללא אימות המשתמש	
***2.3**	ניהול הרשאות המשתמשים יהיה מבוסס תפקיד לפי קבוצת הרשאה ב- Active Directory ובהתאם לעקרון need-to-know בנוסף, המערכת תוודא כי משתמש לא יכול לחרוג מההרשאות הניתנות לו	
***2.4**	המערכת לא תכיל משתמשים גנריים. שימוש במשתמשים אפליקטיביים ב AD בלבד.	
***2.5**	המערכת תכלול מנגנון לאימות קלט/פלט וסינון קבצים. ותכלול מנגנון למניעת שיבוש קבצים (TAMPER RESISTANCE) ברכיבי המערכת	
2.6	במידה וקיימת אפשרות להעלאת קבצים במערכת, על המערכת לוודא את סוג הקובץ המורשה על פי MIME TYPE, בנוסף נדרש לחבר למערכת ההלבנה של ביה"ח. על הספק להגדיר מה ההגבלות הנדרשות (סוג הקבצים, גודל הקבצים). מערכת ההלבנה כוללת השטחת הקובץ.	
2.7	המערכת מחויבת לעבוד רק עם משתמש Service שאורך סיסמתו תהיה לפחות 25 תווים מורכבים ולא יוכל לבצע Login למערכת ההפעלה . תוקף הסיסמא יוגדר 180 ימים.	
***2.8**	טיפול בשגיאות ריצה יטופלו בקוד ולא יוצג למשתמש הקצה. במקרה של תקלה, הודעת השגיאה למשתמש תכיל את המינימום הנדרש בכדי לתפעל את התקלה לדוגמה מספר שגיאה. בכל מקרה, הודעת השגיאה לא תכיל מידע חסוי כמו פרטי משתמשים/מטופלים ו/או מידע רגיש על הגדרות ותהליכים פנימיים של המערכת ושרתי המערכת. בנוסף, במקרה שזוהתה שגיאה אפליקטיבית ובפרט שגיאת אבטחה באפליקציה, יש לנתק מייד את ה session ולתעד בטבלת הלוג.	
***2.9**	יוגדר idle session time-out שלא יעלה על 15 דקות. נדרש לבצע ניתוק session בצד השרת.	

שם ממלא הטופס: _____ חתימה: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

2.10*	ניהול בקרה ותיעוד בטבלת לוג (AUDIT TRAIL): המערכת תיישם מנגנון של רישום לטבלת לוג ותתעד את פעולות המשתמשים והתהליכים במערכת שמתבצעים על ידי המשתמשים האפליקטיביים. מנגנון התיעוד יהיה מוגן מפני שינוי או ביטול של הפעלתו ככל הניתן ויפיץ התראות בהתאם. הלוג יכיל את הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה (timestamp), רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה (קריאה/כתיבה/עדכון וכדומה) , היקפה, ואם הגישה אושרה או נדחתה. התיעוד ישמר ל24 חודשים לפחות. טבלת הלוג תשמר באינסטנס נפרד ממסד נתונים המערכת ותהיה מוגנת מפני מחיקה או שינוי וממודרת בגישה למורשים בלבד.	
2.11	ניטור: המערכת תתמוך בהעברת הלוגים למערכת SIEM מרכזית כדוגמה Qradar	
2.12	אם האפליקציה דורשת חיבור מבחוץ – נדרש להגדיר אימות רב שלבי (MFA). יש לבצע הגבלת ניסיונות גישה/שליחת OTP ברמה אפליקטיבית (Rate Limit) – 10 ניסיונות בטווח זמן של 5 דקות. מעבר לכך יש לחסום את המשתמש ל-15 דקות. או לחלופין להטמיע Google ReCAPTCHa בגרסה עדכנית.	
2.13	אם האפליקציה הינה פנימית – יש לבצע הגבלת ניסיונות לחיבור ל-3 , כאשר לאחר 3 ניסיונות כושלים, ייחסם המשתמש ל-15 דקות.	
2.14	כל התקנת תוכנה תחויב באישור צוות אבטחת מידע, אין להתקין תוכנות ללא אישור	
2.15	תמיכה ברישיון תוכנתי ולא דרך דונגל פיסי	
2.16	לפני כל עדכון לאפליקציה יש לבצע הלבנה לקבצי התקנה בתיאום מראש עם צוות התשתיות (סיסטם ואבטחת מידע)	
2.17*	שם משתמש וסיסמא בעלי הרשאת גישה של Administrator יועברו לנציגי אגף מערכות מידע ודיגיטל	
2.18	ממשק הניהול יהיה מאובטח עם סיסמא מורכבת אורך מדיניות הסיסמה תהיה לפחות 12 תווים המורכב משילוב של לפחות אותיות גדולות + אותיות קטנות + ספרות וסימנים מיוחדים. תיעוד הפעולות המתבצעות בממשק הניהול ישמרו בטבלת הלוג. ממשק ניהול ברשת שיבא לא יהיה מוחצן החוצה – מידור גישה לפי IP פנימי ממשק ניהול בענן יוגבל לגישה לפי IP ארגוני של הספק ושל שיבא. התחברות תתבצע עם אימות רב שלבי. ההתחברות תתבצע ע"י משתמש אדמין ייעודי של העובד ולא עם המשתמש שמבצע לוגין	
2.19	כל סיסמאות ברירת המחדל (של היצרן) ישונו בתשתיות ובאפליקציות	
2.20*	לא יינתנו הרשאות מנהלן על השרתים ו/או התחנות בהן תותקן המערכת (Local Admin)	
2.21	שמירת סיסמאות/מפתחות תתבצע בצורה מוצפנת ולא ב -Clear Text וישמרו במסד הנתונים / Vault	
2.22*	במידה וקיימת אופציית שדרוג/עדכון למערכת מממשק הניהול, הכניסה תתאפשר למורשים בלבד בהתאם להרשאות שייקבעו מראש.	
2.23	יש לבטל חשיפת מידע רגיש ב-Headers , ולהוסיף Security Headers המקובלים ניתן להיעזר בלינקים הבאים : הסרת Headers – https://owasp.org/www-project-secure-headers/ci/headers_remove.json הוספת Headers - https://owasp.org/www-project-secure-headers/ci/headers_add.json	
2.24*	יש לחסום מתודות שלא נמצאות בשימוש כגון: OPTIONS TRACE HEAD PROPFIND COPY LOCK UNLOCK PROPPATCH MKCOL MOVE DELETE	
2.25	יש לבטל את האופציות הבאות: Null ciphers, Anonymous ciphers וביטול חבילת הצפנה RC4	
2.26	ביטול Print Spooler Service	
2.27	ביטול פרוטוקול IPv6	
2.28	הדלקת פרוטוקולים מבוטלים תתבצע רק לאחר אישור צוות אבטחת מידע של בית החולים	
2.29	הסרת Open SSH	

שם ממלא הטופס: _____ חתימה: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר ,מיקוד , 5265601 ישראל

2.30	נא לציין גרסת JQuery (צריכה להיות גרסה עדכנית) : _____	
2.31	הגבלת תיקיית BOOT לקריאה בלבד (LINUX)	
2.32	Token יכיל 20 תווים לפחות ויוצפן במנגנון מוקשח ועדכני. נדרש לוודא את הטוקן בצד שרת.	
2.33	Directory Listing - נדרש לוודא שהתמיכה ב- Directory Listing על ידי שרת ה- Web מנוטרלת (Disabled) עבור כל הספריות תחת ספרייה הראשית של השרת.	
2.34	נדרש לחסום את הגישה לכל תיקיית ה ' git'-ולקבצים שבתוכה. (רלוונטי רק לאתרים שמנוהלים על ידי Open GIT)	
2.35	נדרש להטמיע מנגנון הגנה מפני מתקפות Cross Site Scripting . • יש להשתמש ב- Framework מודרני הכולל הגנה מובנית כנגד פגיעויות XSS . • לוודא שכל שדות הקלט עוברים בדיקה, נטרול תווים בעיתיים (Sanitization) או Escaping הכלל. • מומלץ לבצע Output Encoding כאשר מידע ממשתמש אחד מוצג למשתמש אחר. אם המשתמש נדרש ליכולת להזין קוד HTML למערכת, מומלץ להשתמש ב- HTML Sanitization	
2.36	נדרש להטמיע מנגנון הגנה מפני מתקפות SQL Injection. • מומלץ לא לאפשר בניה דינמית של SQL Query ממידע שהוזן על ידי המשתמש. • מומלץ להשתמש ב- Prepared Statements . • מומלץ להשתמש ב- Properly Constructed Stored Procedures .. • מומלץ להשתמש ב- Allow-list Input Validation . • מומלץ להשתמש ב- Escaping עבור כל קלט המגיע מהמשתמש • ניתן להיעזר באכיפת הרשאות גישה לפי עיקרון Least Privilege	
2.37*	אין להעביר פרטים רגישים במתודת GET . נדרש להעביר במתודת POST עם הצפנה (ניתן להשתמש בהצפנה סטנדרטית SHA256)	

3. <u>דרישות בנושא תקשורת</u>

סעיף	דרישה	מקובל/לא מקובל
3.1	באלו Ports (TCP/UDP) המערכת משתמשת: _____ יש לציין עבור על פורט את השימוש שלו	
3.2*	שימוש בפרוטוקולים מאובטחים בלבד .כגון HTTPS ולא HTTP	
3.3	יוטמעו תעודות מה CA הארגוני SHA2 4096bit	
3.4*	המערכת תוגדר לפעול ללא כל תקשורת ליעדים מחוץ לרשת הארגונית אלא אם ביה"ח הגדיר לה אחרת	

שם ממלא הטופס: _____ חתימה: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר ,מיקוד , 5265601 ישראל

4. דרישות בנושא קישוריות

סעיף	דרישה	מקובל/לא מקובל
4.1	במידה והפתרון יושם ע"י החברה באתר אחר, על הספק לפרט לגבי ההטמעה של המערכת וכן על אופן הקישוריות כפי שבוצע.	
4.2	האם מידע מועבר למערכת קלינית? במידה ומידע מועבר למערכת קלינית יש לציין לאיזו מערכת (כגון: קמיליון, פאקס וכו') _____	
4.3	חיבור ממשקים בצורה מאובטחת ומוצפנת כגון Kerberos, LDAPS , TLS1.2 ומעלה, Updated Cipher Suite	
4.4	המערכת תתחבר מול Active Directory ב LDAPS ו- Kerberos	
4.5	יוטמעו תעודות מה CA הארגוני SHA2 4096bit	
4.6*	תקשורת בין ממשקים ורכיבים פנימיים של המערכת תתבצע באמצעות הזדהות עם משתמש אפליקטיבי ב Active directory הארגוני	
4.7	המערכת חייבת לספק ולתמוך באפשרויות הקישור הבאות (עלויות החיבור תהיינה על הספק): 1. העברת נתונים למערכות קיימות (לדוגמא - תיקים רפואיים, אוטולימס) בהתאם לסטנדרטים מקובלים (FHIR, txt , PDF , Dicom ועוד) 2. קבלת נתונים ממערכות קיימות וטעינתם (לדוגמא - נתוני דמוגרפיה) בשתי צורות אפשריות: 2.1 קבלת קובץ מהמערכת התפעולית לדוגמא קובץ נתוני דמוגרפיה 2.2 שימוש ב-Web Service לצורך קבלת נתוני דמוגרפיה מהמערכת התפעולית	
4.8	העברת נתונים חייבת לתמוך בהעברה מלאה ותכופה (בקצב של נתון בדקה לפחות) של הפרמטרים המוגדרים כחובה על פי הצוות הרפואי.	
4.9	הקישוריות אמורה להיות ניתנת לשינוי ולהתאמה בהתאם לדרישות המרכז הרפואי ולממשקים הקיימים	
4.10	כל המשתמע מביצוע הממשקים למערכות שיבא הינו באחריות החברה ובטיפולה הבלעדי מול ספקיות התוכנה לרבות אפיון הממשקים, פיתוחים הנדרשים מכל הצדדים (כולל ספקי התיק הרפואי ,כגון : iMDsoft ואלעד מערכות, סופטוב) וההוצאות הכספיות בגין העבודה הנדרשת משני הצדדים. במסגרת אפיון הממשקים החברה תתחייב לחשוף את הפרוטוקול איתו היא עובדת.	
4.11*	הצפנת נתונים רגישים תיושם בשימוש אלגוריתם הצפנה חזק	
4.12	אבטחת API הינה באחריות הספק. יש להשתמש במוצר ייעודי לאבטחת בקשות API.	

5. דרישות והנחיות אבטחת מידע

סעיף	דרישה	מקובל/לא מקובל
5.1	אין לחבר מתג, ראוטר, HUB וכל רכיב תקשורת אחר למכשיר/מחשב/שרת ו/או לרשת בית החולים.	
5.2*	ביטול כל תכנה צד ג' של שליטה מרחוק (לדוגמא: TeamViewer , VNC וכו'...)	
5.3*	התחברות למרכז הרפואי שיבא תל השומר לצורכי תמיכה תתבצע ע"י מערכת SSL VPN שיבאי עם אימות דו שלבי ואישור רפרנט מטעם שיבא. על הספק לחתום על טופס סודיות בנספח "סודיות" החיבור יתבצע ממחשב מוקשח של הספק ומכתובת ip קבועה/ישראלית	
5.4*	במידה והמערכת תכיל מידע אישי המוגן בחוק הגנת הפרטיות , היא תעמוד בכל התקנות הנדרשות בחוק, נדרש אישור של ממונה הגנת הפרטיות הארגונית.	
5.5*	נדרש לבצע למערכת מבדקי חדירה ו/או סקרי סיכונים. עליה לאוויר מותנית באישור צוות הגנת הסייבר לאחר תיקון הממצאים.	
5.6	במידה ובוצע מבדק חדירה ו/או סקר סיכונים ע"י הספק, האם ניתן לספק סיכום ממצאים לגורמי הסייבר במרכז הרפואי שיבא? **במידה וקיימים ממצאים פתוחים ברמת סיווג בינוני ומעלה הספק מתחייב לסגור אותם לפני רכישת המוצר על ידי ביה"ח והתחייבות לסגירת הממצאים הנמוכים עד 3 חודשים.**	

שם ממלא הטופס: _____ חתימה: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר ,מיקוד 5265601 ישראל

***5.7**	במידה ותמצא ע"י אגף מערכות מידע ודיגיטל חשיפה/חולשה שתסווג על ידה כקריטית במערכת, מכשיר, מחשב ו/או בשרת המחובר אליו. על הספק/יצרן לדאוג לחסום זאת במידי ולטפל בממצא *סיווג רמת החשיפה/חולשה מתבצע בהתאם להערכת סיכוני אבטחת המידע של בית החולים	
***5.8**	לאחר ביצוע סקר סיכונים ו/או מבדק חדירה, ככל שיימצאו פערים המחייבים התאמות או תיקונים לצורך עמידה בדרישות האבטחה, הספק יישא בעלויות הנדרשות לביצוען, וזאת כחלק מהתחייבותו לספק פתרון מאובטח, ובהתאם לעקרונות הפיתוח המאובטח (Secure Development Lifecycle) אשר מהווים חלק בלתי נפרד מדרישות ההסכם.	
***5.9**	מידע טכני רגיש ישמר בכספת פרטית ולא באחסון ציבורי/של הספק. *מידע טכני רגיש לדוגמה מסמך ארכיטקטורה של המערכת הכולל פרוטוקולים של התקשורת ,פרטי משתמשי המערכת ,קונפגורציות והקשחות הנדרשים מהמערכת	

6. <u>דרישות לחיבור רכיבים נוספים/בקר/ /IOT – למלא רק אם רלוונטי למערכת</u>

סעיף	דרישה	מקובל/לא מקובל
6.1	כל נושא החיבורים מרחוק יבוצע דרך אגף מערכות מידע בלבד ללא תוכנות צד שלישי.	
62	לא יותקן מודם בתחנה ,במידה ומותקן מודם הוא יוסר לפני חיבור לרשת שיבא – באחריות הספק , במידה ויש צורך במודם לתפעול השוטף של המערכת יש לפנות למנהל התפעול.	
6.3	האם קיימים במכשיר/בקר יותר מכרטיס רשת אחד ,אם כן ציינו כמה ולאיזה צורך _____	
6.4	כל עדכון לחומרה ,מערכת ההפעלה ,אפליקציה וכו 'יש לבצע הלבנה לקובצי התקנה בתיאום מראש עם יחידת המחשב.	
6.5	על הספק לספק מחשב/שרת Gateway על מנת לחבר את הבקר לרשת בית החולים. **רכיבים כגון :קפסולות , DIGI ,לנטרוניקס לא מאושרים בבית חולים.**	
6.6	במידה ומידע מועבר למערכת ממוחשבת יש לציין לאיזו מערכת (לדוגמא : בקרת מיזוג, חשמל וכו')	
6.7	התווך לממשק הניהול של הבקר/ציוד iOT יהיה מוצפן (על פי תקן מקובל)	
6.8	כל סיסמאות ברירת המחדל (של היצרן) ישונו בתשתיות ובאפליקציות	
6.9	הסיסמאות הנמצאות בבקר/ציוד iOT לא יהיו ב Clear Text ויישמרו רק בצורה מוצפנת	
6.10	ממשק הניהול יהיה מאובטח עם סיסמא מורכבת	
6.11	הבקר/ציוד iOT יוגדר עם כתובות IP ב VLAN ייעודי ברשת בית החולים (מאחורי Firewall ארגוני) שצוות הגנת הסייבר יספק.	
6.12	אלו (TCP/UDP) Ports המערכת משתמשת: _____	
6.13	בקר/מכשיר/מחשב/שרת שיסופק ,יותקן עליו מערכת הגנה XDR הקיים בארגון ע"י נציגי בית החולים. התמיכה תהיה למערכות הפעלה Windows, Linux, Unix, MAC OS בתמיכת היצרן העדכונים היומיים של האנטי וירוס יבוצעו ע"י שרת הארגוני. א).יש לציין החרגות במידת הצורך_____	
6.14	במידה וסעיף 6.13 "לא מקובל" על היצרן להתקין תוכנת(Application Control (White List המאשרת הפעלת קבצים לפי HASH או לפי. Certificate יש לציין את הפרטים הבאים: שם המערכת _____ :גרסה_____ : ☐ההגנה תוגדר על כל הכוננים הקיימים הכולל חסימה עלDisk on key ☐המוצר ייבדק ע"י נציג צוות הגנת הסייבר(שיבא) ונציג הספק/יצרן. ☐יש לספק מהיצרן סיסמה למערכת ורשימת הקבצים המוחרגת.	
6.15	המכשיר יותקן עם הגבלת רכיבים נתיקים(כגון יציאת USB ו(. CD שדרוגים למערכת/תוכנה ו/או למכשיר יתואמו מראש עם יחידת המחשב לצורכי הלבנת מדיה נתיקה(כגון , Disk on key :דיסק נייד CD ,וכו.)...'	

שם ממלא הטופס: _____ חתימה: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר ,מיקוד , 5265601 ישראל

6.16	במידה ותמצא ע"י יחידת המחשב חשיפה/חולשה קריטית בבקר ,ציוד, iOT מכשיר ,מחשב ו/או בשרת המחובר אליו .על הספק/יצרן לדאוג לחסום זאת במידי.	
6.17	האם בוצע לבקר/ציוד iOT מבדק חדירה או סקר סיכונים ב 18 חודשים האחרונים?	
6.18	במידה ובוצע מבדק חדירה ו/או סקר סיכונים ,האם ניתן לספק סיכום ממצאים לגורמי הסייבר במרכז הרפואי שיבא	
6.19	תמיכה מול שרתי NTP הארגוני – יתרון	
6.20	האם יש מערכת שמאפסת הגדרות לאחר אתחול?	
6.21	האם המכשיר עומד בתקינה כגון HIPAA / ISO 27799 :	
6.22	האם יש רישום לוגים בבקר? נא לציין היכן נרשמים הלוגים ומה סוגי הלוגים: _____ _____	
6.23	האם ליצרן יש הרשאת אדמין על הבקר על מנת לבצע שינויים בבקר	
6.24	האם לספק יש הרשאת אדמין על הבקר על מנת לבצע שינויים בבקר	
6.25	בחתימה על הסכם זה ,הספק מתחייב לעמוד בכל דרישות אבטחת מידע וסייבר על פי המדיניות שתקבע ע"י מרכז הרפואי שיבא והממונה על אבטחת המידע תתעדכן מעת לעת	

7. <u>אפיון דרישות אבטחת מידע לרכיבי AI – למלא רק אם רלוונטי למערכת</u>

סעיף	דרישה	תשובות
7.1	מה סוג המודל ? לדוגמא LLM\ ML\NLP	
7.2	האם המודל רץ מקומית או בענן ?	
7.3	האם נדרשת גישה לכתובות חיצוניות ?	
7.4	איזה מידע קיים במודל ?	
7.5	האם יש בקרת גישה לקבצי המודל ?	
7.6	האם המודל כבר מאומן או שנתוני שיבא ישמשו לאימון המודל ?	
7.7	האם המודל מבוסס על שיתוף המונים ?	
7.8	האם נדרש עיבוד מידע רגיש (PII\PHI)?	
7.9	האם קיים מנגנון שמבצע אנונימיזציה ? ניתן לעבוד עם מידע מותמם או מותמם מדומה ?	
7.10	האם יש מנגנון למניעת prompt injection ? במידה וכן נא לפרט	
7.11	האם קיים מנגנון סינון תוכן ? במידה וכן נא לפרט	
7.12	האם מתבצעות ביקורות תקופתיות על אמינות תוצאות המודל ?	
7.13	האם קיים תהליך ניהול גרסאות ועדכון סדור למודל ?	
7.14	האם קיימת אפשרות במערכת להעברת לוגים למערכת SIEM ?	
7.15	כל העברת נתונים רגישים, עיבודם או אחסונם יבוצעו באמצעות הצפנה בטכנולוגיות העדכניות ביותר.	
7.16	מניעת גישה לא מורשית :השימוש בטכנולוגיות AI מחייב גישה מוגבלת רק לעובדים מורשים בעלי הרשאות מתאימות.	

שם ממלא הטופס: _____ חתימה: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

8. <u>דרישות אבטחת מידע לענן – למלא רק אם רלוונטי למערכת</u>

סעיף	דרישה	תשובות
8.1	האם המערכת תוטמע בענן של שיבא או בענן של חיצוני ? היברידי ?	
8.1.1	ענן חיצוני - תצורת עבודה Multi-Tenant\Single-Tenant ?	
8.1.2	ענן חיצוני - האם המידע של שיבא מאוחסן באזור מבודד?	
8.1.3	ענן חיצוני - האם קיימים מנגנוני הגנה WAF, Anti-DDOS ?	
8.1.4	האם העבודה תתבצע עם משתמשים מקומיים או שניתן להסתמך על IDP של שיבא ?	
8.1.5	האם קיים מנגנון MFA ? (אפליקציה/SMS/מייל/קולי)	
8.2	מי המשתמשים במערכת ? אנשי תשתיות/צוות רפואי/מטופלים	
8.3	איזה מידע מעובד/מאוחסן במערכת ? סיווג.	
8.4	מה מנגנון העברת המידע? API/VPN מאובטח?	
8.5	מה הם מנגנוני האבטחה של Data in transit/Data at rest	

<u>יצירת קשר:</u>

<u>יש לקבל אישור בכתב מהרשומים מטה לנספח זה. ללא אישור זה, הנספח אינו מאושר</u>.

***לכל שאלה/הבהרה ניתן לפנות במייל:** CSTP@sheba.health.gov.il

שם ממלא הטופס: _____ חתימה: _____

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר ,מיקוד , 5265601 ישראל

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

נספח סודיות:

התחייבות לשמירת סודיות ולמניעת ניגוד עניינים-ספק

תאריך : ___/___/_____

לכבוד

המרכז הרפואי ע"ש שיבא, תל השומר

==========

א.ג.נ

הנדון: התחייבות לשמירת סודיות ולמניעת ניגוד עניינים

הואיל המרכז הרפואי ע"ש שיבא, תל השומר (להלן "שיבא") מעוניין לקבל שירותים בנושא _____ עבור יחידת המחשב בשיבא (להלן: "השירותים");

והואיל והמציע_____ (להלן: "המציע) מעוניין להעניק שירותים אלו.

והואיל ושיבא התנה את התקשרות שני הצדדים בתנאי שהמציע והבאים מטעמו ישמרו על סודיות כל המידע כהגדרתו להלן, וכן על סמך התחייבות המציע לעשות את כל הדרוש לשמירת סודיות המידע;

והואיל והוסבר לי כי במהלך עיסוקי במתן השירותים לשיבא ו/או בקשר אליהם יתכן כי אעסוק ו/או אקבל לחזקתי ו/או יבוא לידיעתי מידע מסוגים שונים, שאינו מצוי בידיעת כלל הציבור, בין בעל פה ובין בכתב, בין ישיר ובין עקיף, השייך למזמין ו/או הנודע למזמין ו/או לפעילויותיו בכל צורה ואופן, לרבות אך מבלי לגרוע מכלליות האמור, נתונים, מסמכים ודו"חות (להלן: "המידע");

והואיל והוסבר לי וידוע לי כי גילוי המידע בכל צורה שהיא לכל אדם או גוף מלבדכם, עלול לגרום לכם ו/או לצדדים שלישיים נזק , והוא עלול להוות עבירה פלילית;

שם ממלא הטופס: _____ חתימה: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר ,מיקוד , 5265601 ישראל

אי לזאת, אני הח"מ מתחייב כלפיכם כדלקמן:

1. לשמור על סודיות גמורה ומוחלטת של המידע ו/או כל הקשור והנובע מן השירותים או ביצועם ובפרט מידע הרפואי.
2. ומבלי לפגוע בכלליות האמור בסעיף 1 לעיל, הנני מתחייב כי במשך תקופת מתן השירותים לשיבא או לאחר מכן ללא הגבלת זמן לא אגלה לכל אדם או גוף, לא אפרסם וכן לא אוציא מחזקתי את המידע ו/או כל חומר כתוב אחר ו/או כל חפץ או דבר, בין ישיר ובין עקיף, לצד כלשהוא.
3. מבלי לפגוע בכלליות האמור לעיל, מידע סודי לא יכלול מידע שהינו נחלת הכלל או שהפך להיות נחלת הכלל ללא הפרת חובת הסודיות ו/או מידע שחובה לגלותו על פי כל דין או צו של רשות מוסמכת ו/או מידע שפותח באופן עצמאי ללא תלות במידע הסודי ו/או מידע שהתקבל בידי המציע מצד ג' כדין ללא הפרת חובת סודיות.
4. לנקוט אמצעי זהירות קפדניים ולעשות את כל הדרוש מבחינה בטיחותית, ביטחונית, נוהלית או אחרת כדי לקיים את התחייבויותיי על פי התחייבות זו.
5. להביא לידיעת עובדי ו/או מי מטעמי חובה זו של שמירת סודיות ואת העונש על אי מילוי החובה.
6. להיות אחראי כלפיכם על פי כל דין לכל נזק או פגיעה או הוצאה או תוצאה מכל סוג, אשר יגרמו לכם או לצד שלישי כל שהוא כתוצאה מהפרת התחייבותי זו, וזאת בין אם אהיה אחראי לבדי בגין כל האמור ובין אם אהיה אחראי ביחד עם אחרים.
7. להחזיר לידיכם ולחזקתכם מיד כשאתבקש לכך כל חומר כתוב או אחר או חפץ שקיבלתי מכם או השייך לכם שהגיע לחזקתי או לידי עקב מתן השירותים או שקיבלתי מכל אדם או גוף עקב מתן השירותים או חומר שהכנתי עבורכם. כמו כן, הנני מתחייב לא לשמור אצלי עותק כל שהוא של חומר כאמור או של מידע.
8. שלא לעסוק בכל דרך שהיא בעיסוק שיגרום לי להיות במצב של ניגוד עניינים עם עיסוקי במתן השירותים כאמור לעיל.
9.

שם ממלא הטופס: _____ חתימה: _____

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר ,מיקוד , 5265601 ישראל

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

10. בכל מקרה שאגלה מידע כאמור השייך לכם ו/או הנמצא ברשותכם ו/או הקשור לפעילויותיכם , תהיה לכם זכות תביעה נפרדת ועצמאית כלפי בגין הפרת חובת הסודיות שלעיל.
הנני מצהיר כי ידוע לי ששימוש במידע שיגיע לידי במהלך ביצוע העבודה ומסירתו לאחר מהווים עבירה על פי חוק עונשין, התשל"ז - 1997 וחוק הגנת הפרטיות התשמ"א- 1981 וכן חוקים אחרים לפי סוג המידע, לרבות חוק זכויות החולה, התשנ"ו- 1996.
11. התחייבותי זו לא תפורש כיוצרת קשר אישי מכל סוג שהוא ביני לבניכם.
12. יש למלא פרטי נציג אבטחת מידע של החברה:
    12.1. שם מלא נציג אבטחת מידע מהחברה: _____
    12.2. מייל הנציג: _____
    12.3. מספר סלולרי הנציג: _____

ולראיה באתי על החתום - <u>התחייבות לשמירת סודיות ולמניעת ניגוד עניינים</u>

היום:

_____

יום בחודש שנת

המציע:

_____

שם פרטי ומשפחה ת"ז

_____

כתובת חתימה

שם ממלא הטופס: _____ חתימה: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר ,מיקוד , 5265601 ישראל

טופס הצהרה על שמירת סודיות -עובד של ספק

אני החתום מטה: (שם פרטי ומשפחה) _____ ת.ז: _____

העובד ומועסק אצל _____ (שם המעסיק) , **מתחייב בזאת**:

1. לשמור בסוד ולא להעביר, לא להודיע, לא למסור ו/או לא להביא לידיעת כל אדם, כל ידיעה וכל מידע רגיש ו/או אישי ו/או חסוי לרבות תכנים וחומר בכתב ובעל פה, אשר יגיעו לידיעתי בתקופת עבודתי מטעם _____ (שם המעסיק) הנותן שירותים למרכז הרפואי שיבא תל השומר, בתקופת עבודתי כאמור, או לאחר מכן.
2. התחייבותי זו חלה לגבי כל סוגי המידע, בין אם יגיעו לידיעתי בתוקף עבודתי כאמור ובין אם יגיעו לידיעתי בכל דרך אחרת.
3. ומבלי לפגוע בכלליות האמור בסעיף 1 לעיל, הנני מתחייב כי במשך תקופת מתן השירותים לשיבא או לאחר מכן ללא הגבלת זמן לא אגלה לכל אדם או גוף, לא אפרסם וכן לא אוציא מחזקתי את המידע ו/או כל חומר כתוב אחר ו/או כל חפץ או דבר, בין ישיר ובין עקיף, לצד כל שהוא, לרבות מידע אודות הנבדקים.
4. כמו כן, אני מתחייב כי אם אקבל רשות להשתמש במאגרי המידע של שיבא, אעשה זאת אך ורק לצורך מתן השירותים לשיבא, ובהסכמה מפורשת בכתב מטעם שיבא. אני מתחייב לפעול בהתאם להוראות חוק הגנת הפרטיות והוראות כל חוק הנוגע לעניין.
5. אני מתחייב להתחבר ממחשב השייך לחברה שבה אני עובד ומוגן עם אנטי וירוס מעודכן, לא להוריד מידע ששייך לשיבא למחשבי החברה, אמצעים נתיקים ו/או מחשבים ניידים אלא בכפוף לאישור בכתב מאת ממונה אבטחת המידע של שיבא,
6. אין להעביר את אמצעי הזיהוי החכם שקבלתי משיבא לכל אדם אחר ולא לגלות לאף גורם את הקוד האישי (PIN) המשויך לאמצעי הזיהוי, יש להודיע מידית על אובדן אמצעי הזיהוי או חשיפת הקוד למנהל אבטחת המידע של שיבא.

שם ממלא הטופס: _____ חתימה: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר ,מיקוד , 5265601 ישראל

7. עם סיום עבודתי אצל הספק או עם סיום הצורך בגישה מרחוק מתוקף תפקידי אני מתחייב להודיע על כך למנהל אבטחת המידע של שיבא

8. אני מצהיר בזה שידוע לי, כי אי מילוי התחייבויותיי הנ"ל מהווה עבירה פלילית מכוח חוק העונשין, התשל"ז - 1977 וחוק הגנת הפרטיות התשמ"א-1981 וכן חוקים אחרים לפי סוג המידע, לרבות חוק זכויות החולה, התשנ"ו- 1996 וכי אהיה צפוי לעונשים הקבועים בחוק בגין אי מילוי התחייבויותיי.

9. מספר הסלולרי שאליו אקבל את הקוד: _____

10. דוא"ל ארגוני של העובד: _____

_____ _____

תאריך חתימת המצהיר

שם ממלא הטופס: _____ חתימה: _____