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

נספח 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.
5. נהלי גיבוי ו DR.

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. דרישות בנושא תשתית וארכיטקטורה.

1. **מחשב/שרת** - לרשת בית החולים | Stand Alone | למחשב ייעודי (יש להקיץ בעיגול את המענה)
2. יש לציין את גרסת מערכת ההפעלה: _____
   - 2.1. סוג מערכת הפעלה כגון: (Pro/STD): _____
   - 2.2. יש לציין איזה Service Pack מותקן: _____
   - 2.3. במידה ומותקן נא לציין גרסת OPENSSL: _____
   - 2.4. נא לציין גרסת IIS/Apache במידה ומותקן: _____

סעיף	דרישה	מקובל/לא מקובל
1.1*	המערכת תיישם הפרדה בין שכבת היישום, האפליקציה , לשכבת הנתונים.	
1.2	שרתי בסיסי הנתונים ושרתי ה WEB יהיו נפרדים ולא באותו וילן	
1.3	שרת/מחשב צריך להיות בדומיין שיבא	
1.4	המכשיר הרפואי יחובר ישירות לרשת ביה"ח באמצעות כרטיס רשת (העדפה ל- POE)	
1.5	השרת יותקן וירטואלית תחת VMWARE ESX	
1.6*	השרת יותקן עם מערכת הגנה XDR הקיים בארגון (Sentinel One) ויתעדכן באופן שוטף משרתי ביה"ח	
1.7*	מכשיר/מחשב/שרת שיסופק, יותקן עליו XDR הקיים בארגון ע"י נציגי בית החולים. מערכת הגנה XDR של Sentinel One למערכות הפעלה Windows, Linux, Unix, MAC OS עדכונים של המערכת יבוצעו ע"י שרת הארגוני. 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	
1.8*	במידה וסעיף 1.7 סומן כ "לא מקובל" על היצרן להתקין תוכנת Application Control (**White List**) 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.	
1.9	אם מופעל Firewall מקומי? האם ניתן לבטלו? (הקיפו בעיגול ◯ את התשובה)	כן / לא
1.10	במידה ולא ניתן לבטל Firewall מקומי. יש לבצע כללים (Rules) ב Firewall על פי הנחיית גורם אבטחת מידע בשיבא בזמן הטמעת המוצר.	
1.11	סביבת הייצור, בדיקות, ופיתוח יהיו על גבי שרתים נפרדים. 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	החיבור מרחוק יתבצע דרך מערכת SSL VPN הארגוני וללא תוכנות צד שלישי ומכתובת ip קבועה	
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	מערכת הפעלה תותקן במרכז הרפואי ע"י צוות התשתיות (בשיתוף עם הספק)	

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

1.16	במידה ויידרש מערך אחסון גדול לארכיון השטח יסופק בתצורת NAS , חובה תמיכה בפרוטוקול CIFS **<u>יש לציין את הפרטים הבאים:</u>** 1. גודל השטח שבועי: _____ GB 2. גודל שטח חודשי: _____ GB 3. גודל שטח שנתי: _____ GB	
1.17	תמיכה בעבודה מול האחסון ב Multi Share	
1.18	במידה והמערכת עובדת מול בסיס נתונים, על הספק לתמוך ב SQL 2019 ומעלה	

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. דרישות בנושא אפליקציה והרשאות

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 והמערכת תעבור מבדקי חדירה אבטחתיים לבחינת האבטחה של הקוד הכוללים מבדקי DYNAMIC CODE	
2.2*	המערכת תכלול מנגנון זיהוי ואימות המשתמש בחיבור ל AD, ולא תאפשר כניסה למערכת ללא אימות המשתמש	
2.3*	ניהול הרשאות המשתמשים יהיה מבוסס תפקיד לפי קבוצת הרשאה 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. בנוסף לא ניתן יהיה לבצע לוגין למערכת באמצעותם (הזדהות בתצורת. Login Interactive).	
2.5*	המערכת תכלול מנגנון לאימות קלט/פלט וסינון קבצים. ותכלול מנגנון למניעת שיבוש קבצים (TAMPER RESISTANCE) ברכיבי המערכת	
2.6	האפליקציה מחויבת לעבוד רק עם Service ולא עם User Logon	
2.7	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.	
2.8*	יוגדר session time-out מול המשתמש שלא יעלה על 15 דקות ובפרט בכל ממשקי הניהול של המכשיר שלא יעלה על 10 דקות.	
2.9*	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.	
2.10	אם האפליקציה דורשת חיבור מבחוץ - יש לבצע הגבלת ניסיונות גישה/שליחת OTP ברמה אפליקטיבית – 10 ניסיונות בטווח זמן של 5 דקות. מעבר לכך יש לחסום את המשתמש ל-15 דקות.	
2.11	אם האפליקציה הינה פנימית – יש לבצע הגבלת ניסיונות לחיבור ל-3 , כאשר לאחר 3 ניסיונות כושלים, ייחסם המשתמש ל-15 דקות.	
2.12	Google ReCAPTCHA – ניתן להגביל עד השלמה.	
2.13*	ניטור: המערכת תתמוך בהעברת הלוגים למערכת SEIM מרכזית כדוגמה Qradar	
2.14	כל התקנת תוכנה תחויב באישור צוות אבטחת מידע, אין להתקין תוכנות ללא אישור	
2.15	תמיכה ברישיון תוכנתי ולא דרך דונגל פיסי	

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

2.16	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 הניהול לא יהיה מוחצן החוצה – מידור גישה לפי IP 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	שמירת סיסמאות תתבצע בצורה מוצפנת ולא ב -Clear Text וישמרו במסד הנתונים	
2.21	המערכת תיישם מנגנון הגנה בעדכון גרסה באמצעות תהליך הזדהות נוסף של המשתמש ומידור הגישה למנגנון העדכון בהתאם למורשים בלבד	
2.22*	יש לבטל חשיפת מידע רגיש ב-Headers דוגמה X-Powered-By (שפת השרת + גרסה) ככלל הודעות שגיאה לא יחשפו מידע רגיש על שרתי המערכת	
2.23	יש לוודא ש-HSTS Header מוגדר	
2.24*	יש לחסום מתודות שלא נמצאות בשימוש כגון: OPTIONS TRACE HEAD PROPFIND COPY LOCK UNLOCK PROPPATCH MKCOL MOVE DELETE	
2.25	לבטל את האופציות הבאות: Anonymous ciphers ,Null ciphers וביטול חבילת הצפנה RC4	
2.26	ביטול Print Spooler Service	
2.27	ביטול פרוטוקול IPv6	
2.28	הסרת Open SSH	
2.29	נא לציין גרסת JQuery: _____	
2.30	הגבלת תיקיית BOOT לקריאה בלבד	
2.31	Token יכיל 13 תווים וסיסמתו תוצפן	

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

3. דרישות בנושא תקשורת

סעיף	דרישה	מקובל/לא מקובל
3.1	באלו Ports (TCP/UDP) המערכת משתמשת: _____ יש לציין עבור על פורט את השימוש שלו	
3.2	יש למחוק ב IIS את ה BIND עם פורט 80	
3.3*	שימוש בפרוטוקולים מאובטחים כגון HTTPS ולא HTTP	
3.4	יוטמעו תעודות מה CA הארגוני SHA2 4096bit	
3.5*	המערכת תוגדר לפעול ללא כל תקשורת ליעדים מחוץ לרשת הארגונית אלא אם ביה"ח הגדיר לה אחרת	

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 (Dicom , PDF , txt , XML7HL בצילומים 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 וב סרוויס 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 ב Data in transit ו Data at rest תיושם בשימוש אלגוריתם הצפנה חזק	

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. דרישות והנחיות אבטחת מידע נוספות

סעיף	דרישה	מקובל/לא מקובל
5.1	עבור כל עדכון לחומרה, מערכת ההפעלה, אפליקציה וכו' יש לבצע הלבנה לקובצי התקנה בתיאום מראש עם אגף מערכות מידע ודיגיטל	
5.2	אין לחבר מתג, ראוטר, HUB וכל רכיב תקשורת אחר למכשיר/מחשב/שרת ו/או לרשת בית החולים.	
5.3*	ביטול כל תכנה צד ג' של שליטה מרחוק (לדוגמא: TeamViewer , VNC וכו'...)	
5.4*	התחברות למרכז הרפואי שיבא תל השומר לצורכי תמיכה תתבצע ע"י מערכת SSL VPN 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	
5.5*	במידה והמערכת תכיל מידע אישי המוגן בחוק הגנת הפרטיות , היא תעמוד בכל התקנות הנדרשות בחוק	
5.6	האם בוצע למערכת מבדק חדירה ו/או סקר סיכונים ב 18 חודשים האחרונים?	
5.7*	במידה ובוצע מבדק חדירה ו/או סקר סיכונים, 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**.	
5.8*	במידה ותמצא ע"י אגף מערכות מידע ודיגיטל חשיפה/חולשה שתסווג על ידה כקריטית במכשיר, 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	
5.9	מידע טכני רגיש ישמר בכספת לא באתרים כגון GITHUB *מידע טכני רגיש לדוגמה מסמך ארכיטקטורה של המערכת הכולל פרוטוקולים של התקשורת ,פרטי משתמשי המערכת ,קונפגורציות והקשחות הנדרשים מהמערכת	