

## נספח: דרישות מחשוב והגנת הסייבר להכנסת מכשיר,

### בקר, בקר תעשייתי (SCADA) וציוד IoT לרשת שיבא

מספר מכרז: \_\_\_\_\_ תאריך: \_\_\_\_\_  
 מהות הבקר: \_\_\_\_\_ שם היצרן: \_\_\_\_\_  
 דגם הבקר: \_\_\_\_\_ שם הספק: \_\_\_\_\_  
 שם ממלא הטופס: \_\_\_\_\_ סולרי: \_\_\_\_\_  
 מייל ממלא הטופס: \_\_\_\_\_ @ \_\_\_\_\_

#### דרישות סף:

- סעיפים עם כוכבית (\*) – יש לסמן "מקובל" בנספח.
- מערכות הפעלה נמצאות בתמיכת יצרן מערכות הפעלה.
- מערכות הפעלה מקבלות עדכוני אבטחה באופן שוטף בהתאם למדיניות הארגון.
- מכשיר/מחשב שיוגדר ע"י הספק כ Stand Alone מחויב לקבל אישור ע"י המחלקה/מכון/הנדסה/סדנא ויצורף לנספח מחשוב זה.
- מחשב/מכשיר/בקר שהוגדר כ Stand Alone אינו יורשה להעביר נתונים לרשת בית החולים, למערכות שונות, אחסון וכדומה.

**נספח מכשיר/בקר:**

נא להקיף בעיגול:

- מחובר - לרשת בית החולים | Stand Alone | למחשב ייעודי
- שומר נתונים - מקומית בלבד | באחסון מרכזי | לא שומר
- בשימוש - משקי | מעבדתי | טיפולי/דיאגנוסטי | להתנסות זמנית
- גישה למכשיר לצורכי תחזוקה וטיפול - מהארץ | חו"ל | אין צורך

1. יש לציין את מערכת הפעלה: \_\_\_\_\_
- 1.1 גרסת מערכת הפעלה: \_\_\_\_\_
- 1.2 גרסת Firmware/Software/Kernel: \_\_\_\_\_
- 1.3 סוג מערכת הפעלה כגון (Pro/Embedded): \_\_\_\_\_
- 1.4 יש לציין איזה Service Pack/Patch מותקן: \_\_\_\_\_
- 1.5 במידה ומותקן נא לציין גרסת OPENSSL: \_\_\_\_\_

מקובל	לא מקובל
x	

ממ X בכל משבצת בטבלה, דוגמא -

מס"ד	מקובל	לא מקובל
2		שם משתמש וסיסמא בעלי הרשאת גישה של Administrator יועברו ליחידת המחשב ע"מ לבצע תחזוקה שוטפת.
3		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.
4		כל נושא החיבורים מרחוק יבוצע דרך יחידת המחשב בלבד ללא תוכנות צד שלישי.
5		האם קיימים במכשיר/בקר יותר מכרטיס רשת אחד, אם כן ציינו כמה ולאיזה צורך _____
*6		כל עדכון לחומרה, מערכת הפעלה, אפליקציה וכו' יש לבצע הלבנה לקובצי התקנה בתיאום מראש עם יחידת המחשב.

### נספח מחשב המחובר למכשיר/בקר ו/או לרשת בית החולים

(ימולא עבור מערכות שמחשב והבקר לא יחידה אחת):

נא להקיף בעיגול:

- **מחובר** - לרשת בית החולים | Stand Alone | למכשיר ייעודי
- **שומר נתונים** - מקומית בלבד | באחסון מרכזי | לא שומר
- **בשימוש** – משקי | מעבדתי | טיפולי/דיאגנוסטי | להתנסות זמנית
- **גישה למכשיר/בקר לצורכי תחזוקה וטיפול** – מהארץ | חו"ל | אין צורך

1. יש לציין את מערכת הפעלה: \_\_\_\_\_
- 1.1. גרסת מערכת הפעלה: \_\_\_\_\_
- 1.2. גרסת Firmware/Software/Kernel: \_\_\_\_\_
- 1.3. סוג מערכת הפעלה כגון (Pro/Embedded): \_\_\_\_\_
- 1.4. יש לציין איזה Service Pack/Patch מותקן: \_\_\_\_\_
- 1.5. במידה ומותקן נא לציין גרסת OPENSSL: \_\_\_\_\_

מקובל	לא מקובל
x	

סמן x בכל משבצת בטבלה, דוגמא -

מס"ד	מקובל	לא מקובל
2		שם משתמש וסיסמא בעלי הרשאת גישה של Administrator יועברו ליחידת המחשב ע"מ לבצע תחזוקה שוטפת.
3		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 אבטחת מידע הארגוני.
4		כל נושא החיבורים מרחוק יבוצע דרך יחידת המחשב בלבד ללא תוכנות צד שלישי.
5		האם קיימים במחשב יותר מכרטיס רשת אחד, אם כן ציינו כמה ולאיזה צורך _____
6		כל עדכון לחומרה, מערכת הפעלה, אפליקציה וכו' יש לבצע הלבנה לקובצי התקנה בתיאום מראש עם יחידת המחשב.



**נספח סיסטם ושרתים:**

1. יש לציין את גרסת מערכת ההפעלה: \_\_\_\_\_
- 1.1. סוג מערכת הפעלה כגון: (Pro/STD): \_\_\_\_\_
- 1.2. יש לציין איזה Service Pack מותקן: \_\_\_\_\_
- 1.3. במידה ומותקן נא לציין גרסת OPENSLL: \_\_\_\_\_
- 1.4. נא לציין גרסת IIS/Apache במידה ומותקן: \_\_\_\_\_

סמן X בכל משבצת בטבלה, דוגמא -

מקובל	לא מקובל
X	

מס"ד	מקובל	לא מקובל	
2			השרת יותקן וירטואלית תחת VMWARE ESX .
3			מערכת הפעלה תותקן במרכז הרפואי ע"י הצוות של יחידת המחשב (ביחד עם הספק)
4			במידה ויידרש מערך אחסון גדול לארכיון השטח יסופק בתצורת NAS , חובה תמיכה בפרוטוקול CIFS <b>יש לציין את הפרטים הבאים:</b> 1. גודל השטח שבועי: _____ GB 2. גודל שטח חודשי: _____ GB 3. גודל שטח שנתי: _____ GB
5			תמיכה ברישיון תוכנתי ולא דרך דונגל פיסי .
6			תמיכה בעבודה מול האחסון ב Multi Share
7			במידה והמערכת עובדת מול בסיס נתונים, על הספק לתמוך ב SQL 2016.
8			האפליקציה מחויבת לעבוד רק עם Service ולא עם User Logon .
9			בקר/מכשיר/מחשב/שרת שיוספק, יותקן עליו מערכת הגנה XDR של חברת סנטינל1 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. (. יש לציין החרגות במידת הצורך _____
10			כל עדכון לחומרה, מערכת ההפעלה, אפליקציה וכו' יש לבצע הלבנה לקובצי התקנה בתיאום מראש עם יחידת המחשב.

מקובל	לא מקובל
x	

סמן X בכל משבצת בטבלה, דוגמא -

### קישוריות:

מס"ד	מקובל	לא מקובל	
1		המערכת חייבת לספק ולתמוך באפשרויות הקישור הבאות (עלויות החיבור תהיינה על הספק): (a) העברת נתונים למערכות קיימות (מערכות בקרה של סדנה/הנדסה) בהתאם לסטנדרטים מקובלים	
2		הקישוריות אמורה להיות ניתנת לשינוי ולהתאמה בהתאם לדרישות המרכז הרפואי ולממשקים הקיימים	
3		כל המשתמע מביצוע הממשקים למערכות שיבא הינו באחריות החברה ובטיפול הבלעדי מול ספקיות התוכנה לרבות אפיון הממשקים, פיתוחים הנדרשים מכל הצדדים וההוצאות הכספיות בגין העבודה הנדרשת משני הצדדים. במסגרת אפיון הממשקים החברה תתחייב לחשוף את הפרוטוקול איתו היא עובדת.	
4		הבקר ו/או ציוד IoT יחובר ישירות לרשת ביה"ח באמצעות כרטיס רשת (העדפה ל- POE).	
5		במידה והפתרון יושם ע"י החברה באתר אחר, על הספק לפרט לגבי ההטמעה של המערכת וכן על אופן הקישוריות כפי שבוצע.	
6		על הספק לספק מחשב/שרת Gateway על מנת לחבר את הבקר לרשת בית החולים. <b>רכיבים כגון: קפסולות, DIGI, לנטרוניקס לא מאושרים בבית חולים.</b>	
7	כן	לא	האם מידע מועבר למערכת ממוחשבת?
8	***	***	במידה ומידע מועבר למערכת ממוחשבת יש לציין לאיזו מערכת (לדוגמא: בקרת מיזוג, בקרת חשמל וכו' ...)

**נספח הגנת הסייבר:**

מס"ד	מקובל	לא מקובל	
*1		התווך לממשק הניהול של הבקר/ציוד IoT יהיה מוצפן (על פי תקן מקובל)	
2		כל סיסמאות ברירת המחדל ( של היצרן ) ישונו בתשתיות ובאפליקציות	
*3		הסיסמאות הנמצאות בבקר/ציוד IoT לא יהיו ב ( Clear Text רק בצורה מוצפנת).	
4		ממשק הניהול יהיה מאובטח עם סיסמא מורכבת.	
5	כן	לא	האם מותקן ומופעל Firewall מקומי? (הקיפו בעיגול <input type="radio"/> את התשובה )
6	כן	לא	האם ניתן לבטל את ה - Firewall המקומי ? (הקיפו בעיגול <input type="radio"/> את התשובה )
*7		הבקר/ציוד IoT יוגדר עם כתובות IP בווילן (VLAN) ייעודי ברשת בית החולים ( מאחורי Firewall ארגוני) שצוות הגנת הסייבר יספק.	
8		אלו Ports (TCP/UDP) המערכת משתמשת: _____	
*9		בקר/מכשיר/מחשב/שרת שיסופק, יותקן עליו מערכת הגנה XDR של חברת סנטינל1 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 _____	
*10		במידה וסעיף 9 "לא מקובל" על היצרן להתקין תוכנת Application Control (White List) המאשרת הפעלת קבצים לפי HASH או לפי Certificate. <b><u>יש לציין את הפרטים הבאים:</u></b> שם המערכת: _____ גרסה: _____	
11		המוצר ייבדק ע"י נציג צוות הגנת הסייבר (שיבא) ונציג הספק/יצרן. יש לספק מהיצרן סיסמה למערכת ורשימת הקבצים המוחרגת. 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'...).	

**המשך נספח הגנת הסייבר:**

מס"ד	מקובל	לא מקובל	
12		כל פורט נוסף אשר אינו משמש לתקשורת והפעלת הבקר/ציוד IoT באופן קבוע ייחסם ע"י הספק ברמת מערכת הפעלה או ברמה פיזית.	
13		אין לחבר מתג, ראوتر, HUB וכל רכיב תקשורת אחר למכשיר/מחשב/שרת ו/או לרשת בית החולים.	
*14		ביטול כל תכנה צד ג' של שליטה מרחוק (לדוגמא: TeamViewer, VNC וכו'...) , ניתן להשתמש בתוכנות פנימיות של ביה"ח משרת ספקים למכשיר הרפואי.	
*15		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.	
16		הכנסת מחשב/שרת לדומיין	
*17		על הספק לחתום על טופס סודיות בנספח "סודיות"	
18		המחשב/שרת יקבל עדכוני אבטחה של מיקרוסופט באופן שוטף.	
19		האם בוצע לבקר/ציוד IoT מבדק חדירה או סקר סיכונים ב 18 חודשים האחרונים?	
20		במידה ובוצע מבדק חדירה ו/או סקר סיכונים, האם ניתן לספק סיכום ממצאים לגורמי הסייבר במרכז הרפואי שיבא	
21		תמיכה מול שרתי NTP הארגוני – יתרון	
22		מסמך הגדרות של היצרן הכולל התקנה מפורטת של ה – Certificates יתרון	
23	כן	לא	האם יש מערכת שמאפסת הגדרות לאחר אתחול?
24	כן	לא	האם המכשיר עומד בתקינה כגון: HIPAA / ISO 27799

**נספח תקשורת ורשת אלחוטית:**

מס"ד	מקובל	לא מקובל	
*1		<p>חיבור לרשתות אלחוטיות על פי תקן (הקיפו בעיגול) <input type="radio"/> את התקן הקיים אצלכם)</p> <p>א. 802.11ac (wave2)          ב. 802.11n</p>	
*2		<p>יכולת התקנת תעודת אבטחה ( User Certificate/Computer Certificate )          בעדיפות ל- Computer Certificate</p> <p>As per hospital policy we allow wireless access to internal network with 802.1x (based on certificates only).          Encryption – WPA2-AES (WPA2 with AES encryption and dynamic keys using 802.1x via Transport Layer Security (TLS)).          Support cryptographic hash function (Secure Hash Algorithm 2) <b>SHA2</b>.</p>	
3		ניהול מרחוק (הטמעה ועדכון תעודות הצפנה ושינוי הגדרות)	
4		חסימת גישה בBluetooth	
5		תמיכה בשרתי NTP הארגוני – יתרון	
6		עדכון/חידוש תעודות Certificate באופן אוטומטי – יתרון	
7	כן	לא	האם מופעל שידור במולטיקאסט (רב-נתיב)
8			אישור כרטיס ה WIFI מותנה בבדיקה פיזית במרכז הרפואי שיבא



**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;

### 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 התחייבויותי 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 שיגרור לי להיות במצב של ניגוד עניינים עם עיסוקי במתן השירותים כאמור לעיל.
9. 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.
10. התחייבותי זו לא תפורש כיוצרת קשר אישי מכל סוג שהוא ביני לביניכם.

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

**ולראיה באתי על החתום - התחייבות לשמירת סודיות ולמניעת ניגוד עניינים**

היום:

יום בחודש שנת

המציע:

שם פרטי ומשפחה ת"ז

כתובת

חתימה

## התחייבות לשמירת סודיות לחתימת העובדים של ספק

תאריך: \_\_\_\_/\_\_\_\_/\_\_\_\_

אני החתום מטה, \_\_\_\_\_, ת.ז. \_\_\_\_\_, (שם פרטי ושם

משפחה) העובד מועסק 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, אשר יגיעו לידיעתי בתקופת עבודתי מטעם \_\_\_\_\_ (שם המעסיק) הנותן שירותים ל \_\_\_\_\_, 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 מצהיר בזה שידוע לי, כי אי מילוי התחייבויותי 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 התחייבויותי.

6. מספר הסולרי שאליו אקבל את הקוד: \_\_\_\_\_

7. דוא"ל ארגוני של העובד: \_\_\_\_\_

**\*לכל שאלה/הבהרה ניתן לפנות במייל: [infosec@sheba.health.gov.il](mailto:infosec@sheba.health.gov.il)**

**רומן קורוביצין 054-3358913 רומן רטמן: 054-6975739 איתמר אדות 050-3562572**

**בכל תצורה אחרת יש לקבל מראש אישור מנהל צוות תקשורת והגנת הסייבר**