מבחנים לחלוקת כספי תמיכות של משרד הבריאות לצורך הקמת תשתית FHIR בקופות החולים

לפי חוק יסודות התקציב, התשמ"ה-1985

בהתאם לסעיף 3א לחוק יסודות התקציב, התשמ"ה-1985[1] (להלן – **החוק**), ובהתייעצות עם היועץ המשפטי לממשלה, מתפרסמים בזה מבחנים לחלוקת כספי תמיכות של משרד הבריאות (להלן – **המשרד**) לצורך הקמת תשתית FHIR בקופות החולים, כמפורט להלן:

תקנה תקציבית מספר: 04521521

1. כללי

(א) ועדת התמיכות של המשרד (להלן – **הוועדה**) תדון בעניין תמיכה מתקציב המשרד לפי הנוהל להגשת בקשות לתמיכה מתקציב המדינה במוסדות ציבור[2] (להלן – **הנוהל**).

(ב) התמיכה עצמה צריך שתינתן, אם אכן נכון וראוי לתתה, על פי עקרונות של סבירות ושוויון בין מקבלי התמיכה השונים.

(ג) בבואה לדון ולהחליט בכל בקשה לתמיכה, תשקול הוועדה את כל נסיבותיו של העניין, תוך יישום שוויוני, אחיד ועניני של המבחנים שנקבעו.

(ד) כל שיקוליה של הוועדה יהיו עניינים, תוך הפעלת אמות מידה מקצועיות, ככל שיידרש לפי נסיבות העניין; הוועדה תנמק את החלטותיה.

2. הגדרות

במבחנים אלה –

"**ארגון בריאות**" – קופת חולים, בית חולים, ארגוני פינוי והצלה, שירותי הרפואה של צבא ההגנה לישראל ושל שירות בתי הסוהר, משרד הבריאות ויחידותיו;

"**משתמש פעיל**" – מבוטח של קופה העושה שימוש באפליקציה שהוטמעה בקופה, במהלך 3 חודשים רצופים, בהתאם לאופי האפליקציה;

"**ספק משמעותי**" – ספק שירות רפואי אשר נמצא בהתקשרות עם קופת חולים לתקופה של שנה לפחות, ואשר מספק שירות רפואי לארגון בריאות נוסף אחד לפחות, עבור למעלה מ-500 מטופלים בחודש בסך הכל; לדוגמא – בית חולים, מכון דימות, מרכז בריאות הנפש;

"**קופת חולים**" – כהגדרתה בחוק ביטוח בריאות ממלכתי, התשנ"ד-1994[3];

"**FHIR**" – תקן בין לאומי להחלפה ושיתוף מידע בין מערכות וארגונים בתחום הבריאות המפותח על ידי ארגון HL7 המפורסם בכתובת: http://hl7.org/fhir/;

"**FHIR IL**" – התאמה מקומית של תקן FHIR עבור מערכת הבריאות הישראלית, המפותחת על ידי קהילת FHIR-IL;

SMART on FHIR – חלק מתקן FHIR המשמש כתקן לחיבור אפליקציות צד ג' לתיק הקליני, המפורסם בכתובת: http://www.hl7.org/fhir/smart-app-launch/.

3. הגופים הנתמכים

הגופים הנתמכים לפי מבחנים אלה הינם קופות החולים.

4. מטרת התמיכה

מטרת התמיכה לפי מבחנים אלה היא הקמת תשתית FHIR שתאפשר סטנדרטיזציה בממשקי המידע הקיימים בין קופות החולים והמטופלים ובין קופות החולים וספקי הקופות, ותסייע בהטמעת חדשנות וכלים טכנולוגיים במערכת הבריאות.

---

[1] ס"ח התשמ"ה, עמ' 60; התשנ"ב, עמ' 34.
[2] י"פ התש"ף, עמ' 482 ו-7207; התשפ"א, עמ' 2, 1732, 3640 ו-3774.
[3] ס"ח התשנ"ד, עמ' 156.

5. תנאי סף למתן התמיכה

תמיכה לפי מבחנים אלה תינתן לקופת חולים שהתקיימו לגביה כל התנאים האלה:

(1) הקופה משתתפת באופן פעיל ושוטף בקבוצות עבודה רלוונטיות של קהילת FHIR IL לצורך מימוש הפרויקט ומשתפת תוצרים עם הקהילה בהתאם לדרישות המשרד;

(2) הקופה מינתה נציג מטעמה האחראי על העבודה השוטפת מול משרד הבריאות עבור כל אחד מהפרויקטים הנתמכים באמצעות מבחנים אלה;

(3) הקופה מדווחת באופן קבוע ובהתאם לדרישות המשרד על אודות התקדמות תכנית העבודה בכל אחד מהפרויקטים;

(4) הקופה עומדת בנהלי אבטחת המידע והסייבר של משרד הבריאות, נוהל פיתוח מערכות מאובטחות ונוהל אבטחת תשתיות וכן עומדת בתנאי התוספת למבחנים אלה.

6. סכום התמיכה ואופן חלוקתה

תמיכה לפי מבחנים אלה תחולק לשלושה פרקים כמפורט להלן –

(א) **פרק א' – שלב התכנון**

(1) **חלוקת התמיכה – 10% מהתמיכה יחולק עבור תכנון הפרויקט** (בניית אסטרטגיה לקופה, מינוי צוות מוביל והכשרתו, אישור תכנית עבודה מפורטת);

(2) **הפעילות הנתמכת** –

(א) מינוי צוות FHIR ייעודי (להלן – **צוות FHIR**) בקופת החולים, לצורך מימוש הפעילות הנתמכת במבחן התמיכה, והכשרתו בסטנדרט FHIR;

(ב) גיבוש אסטרטגיית FHIR עבור קופת החולים, וגיבוש תכנית עבודה למיפוי נתוני הקופה לסטנדרט FHIR IL ולמימוש ארכיטקטורת הפעילות הנתמכת במבחן זה;

(3) **תנאים לפעילות הנתמכת** –

(א) הגשת התחייבות חתומה של קופת החולים על ידי מנכ"ל הקופה, לקחת חלק פעיל באופן שוטף בכל קבוצות העבודה הרלוונטיות לאפיון הפרויקט, ולשתף את קבוצות העבודה בתכנים רלוונטיים בהתאם לדרישות המשרד;

(ב) חברי צוות FHIR ומנהל הצוות ימונו על ידי מנכ"ל קופת החולים, ושמות חברי הצוות יועברו למשרד; על הצוות לכלול לכל הפחות מנתח מערכות, מפתח אינטגרציה, ארכיטקט נתונים, ואיש צוות מהתחום הקליני או האינפורמטיקה הרפואית, או בעלי תפקידים עם אחריות מקבילה בקופה; חברי הצוות יועסקו לכל הפחות ב-50% משרה בקידום הפעילות הנתמכת במבחן תמיכה זה; בנוסף, יוגדר גורם ייעודי מתחום אבטחת המידע שילווה את הצוות;

(ג) הגשת מסמך אסטרטגיית FHIR בהתאם לדרישות המשרד, ואישורו על ידי המשרד, הכולל התייחסות לנושאים הבאים: מטרות הקמת תשתית ה-FHIR, תרחישי השימוש המרכזיים בהם התשתית מיועדת לתמוך, המידע שיונגש בסטנדרט FHIR באמצעות התשתית, ניתוח המיפוי הטרמינולוגי והשירות הנדרש לניהול טרמינולוגיה, ניתוח סוגיות מרכזיות בארכיטקטורה שנבחרה לתשתית, ניתוח סיכוני פרטיות ואבטחת מידע מרכזיים והפתרונות המוצעים לגידורם, ומבנה ארגוני להובלת הפרויקט בקופה;

(ד) הגשת תעודה המעידה על השלמת הכשרת FHIR לחברי צוות FHIR: HL7 FHIR (R4) Proficiency Certificate או הכשרה אחרת שאושרה על ידי המשרד;

(ה) הגשת תכנית עבודה מפורטת עד לתאריך שיפורסם באתר המשרד, הכוללת התייחסות ללוחות זמנים ותקציב ואישורה על ידי המשרד; התכנית תחולק ל-2 אבני דרך תקציביות, לפיהן תינתן התמיכה באבן הדרך הראשונה והשנייה בפרק ב' (להלן – **אבני הדרך**

התקציביות), וכן תכנית עבודה לכל יתר אבני הדרך המופיעות בפרקים ב ו-ג' ; תכנית העבודה תכלול:

(1) התייחסות לאפיון משאבי ה-FHIR IL כפי שיוגדרו על ידי המשרד, ומשאבי ה- FHIR IL הנדרשים לצורך ביצוע הפרויקטים בפרקים ב' ו-ג' (להלן – **הפרויקטים**) ;

(2) התייחסות למיפוי הטרמינולוגי הנדרש בין הטרמינולוגיות הפנימיות שנמצאות בשימוש בקופה ובין הטרמינולוגיות הסטנדרטיות, כפי שתוגדרנה במשאבי ה-FHIR IL הנדרשים לפרויקטים ;

(3) התייחסות מפורטת למימוש ארכיטקטורת שיתוף מידע מבוססת FHIR ולסוגיות אבטחת מידע ופרטיות לצורך ביצוע הפרויקטים בפרקים ב' וג' ;

(4) **אופן החלוקה** – סכום התמיכה שיעמוד לחלוקה עבור פרק זה יחולק בהתאם לעמידה באבני הדרך, שווה בשווה בין קופות החולים שעמדו באותה אבן דרך ;

(5) **אבני דרך** –

(א) **אבן דרך ראשונה** – במסגרתה יועברו 5% מסכום התמיכה המרבי לחלוקה בפרק זה, תכלול: מינוי צוות FHIR והגשת התחייבות חתומה על ידי מנכ"ל הקופה לקחת חלק פעיל בקבוצות העבודה ולשתף בתוצרי העבודה ;

(ב) **אבן דרך שניה** – במסגרתה יועברו 20% מסכום התמיכה המרבי לחלוקה בפרק זה, תכלול: הגשה ואישור של מסמך אסטרטגיה מאושר על ידי מנכ"ל הקופה בהתאם לדרישות המשרד ;

(ג) **אבן דרך שלישית** – במסגרתה יועברו 40% מסכום התמיכה המרבי לחלוקה בפרק זה, תכלול: הגשה ואישור של תכנית עבודה מפורטת המתייחסת למיפוי נתוני הקופה לסטנדרט FHIR IL ולמיפוי הטרמינולוגי הנדרש ;

(ד) **אבן דרך רביעית** – במסגרתה יועברו 25% מסכום התמיכה המרבי לחלוקה בפרק זה: הגשה ואישור תכנית עבודה מפורטת המתייחסת למימוש הארכיטקטורה ;

(ה) **אבן דרך חמישית** – במסגרתה יועברו 10% מסכום התמיכה המרבי לחלוקה בפרק זה, תכלול: הגשת תעודה המעידה על השלמת הכשרת FHIR בהתאם לסעיף 6, סעיף קטן (א), פסקה (3) פסקת משנה (ד) ; למען הסר ספק, ניתן לשלם את אבן דרך החמישית לאחר ביצועה ללא קשר לעמידה באבני דרך האחרות.

(ב) **פרק ב' – שלב היישום**

(1) **חלוקת התמיכה** – 50% מהתמיכה יחולק עבור שלב היישום (יישום התכנית למיפוי נתונים ל-FHIR, הטמעת שרת FHIR עובד בקופה, אינטגרציה עם ספק משמעותי, והקמת SANDBOX) ;

(2) **הפעילות הנתמכת** – התקנת שרת FHIR והנגשת נתוני הקופה באמצעותו בסטנדרט FHIR IL בהתאם לתכניות העבודה שאושרו בפרק א' ;

(3) **תנאים לפעילות הנתמכת** –

(א) שרת FHIR זמין בסביבת ייצור, העובד לפי הארכיטקטורה שאושרה בתכנית העבודה, והמנגיש את משאבי FHIR IL בהתאם לתכנית העבודה המאושרת ;

(ב) תחזוקת טבלאות המרה מטרמינולוגיות פנימיות לטרמינולוגיות סטנדרטיות וחשיפתן דרך שרת טרמינולוגיה נגיש לכלל צרכני המידע ;

(ג) פרסום דוקומנטציה מלאה של האופן בו ניתן לתשאל את שרת ה-FHIR בהתאם לדרישות המשרד ;

(ד) הקמה ותחזוקה של sandbox פתוח הנגיש למפתחים בהתאם לדרישות המשרד, ובו מידע המדמה את המידע הקיים בשרת FHIR בסביבת הייצור של הקופה ;

(ה) השלמת מימוש אינטגרציה של הקופה ב-FHIR עם לפחות ספק משמעותי אחד של הקופה שאושר על ידי המשרד, הכוללת העברת מידע בסטנדרט FHIR ומתן שירות רפואי הנעזר במידע שהועבר;

(4) **אופן חלוקה** – סכום התמיכה שיעמוד לחלוקה בעבור פרק זה יחולק שווה בשווה בין קופות החולים אשר הגישו תכניות עבודה במועד כאמור בסעיף 6, סעיף קטן (א) פסקה (3) פסקת משנה (ה), בהתאם לאבני הדרך;

(5) **<u>אבני דרך</u>** –

(א) **אבן דרך ראשונה** – במסגרתה יועברו 20% מסכום התמיכה המרבי לחלוקה בפרק זה, תכלול: עמידה באבן הדרך התקציבית הראשונה שבתכנית העבודה;

(ב) **אבן דרך שניה** – במסגרתה יועברו 20% מסכום התמיכה המרבי לחלוקה בפרק זה, תכלול: עמידה באבן הדרך התקציבית השנייה שבתכנית העבודה;

(ג) **אבן דרך שלישית** – במסגרתה יועברו 20% מסכום התמיכה המרבי לחלוקה בפרק זה, תכלול:

(1) התקנת שרת FHIR והעמדת היכולת להנגיש את כלל משאבי ה-FHIR בהתאם לתכניות העבודה המאושרת;

(2) תחזוקת טבלאות המרה מטרמינולוגיות פנימיות לטרמינולוגיות סטנדרטיות וחשיפתן דרך שרת טרמינולוגיה נגיש לכלל צרכני המידע;

(3) פרסום דוקומנטציה המפרט את האופן בו ניתן לתשאל את השרת;

(ד) **אבן דרך רביעית** – במסגרתה יועברו 20% מסכום התמיכה המרבי לחלוקה בפרק זה, תכלול: הקמת sandbox בהתאם לתכנית העבודה המאושרת;

(ה) **אבן דרך חמישית** – במסגרתה יועברו 20% מסכום התמיכה המרבי לחלוקה בפרק זה, תכלול: אינטגרציה של הקופה עם ספק משמעותי על גבי תשתית ה-FHIR בהתאם לתכנית העבודה המאושרת; למען הסר ספק, ניתן לשלם את אבן הדרך החמישית גם בטרם ביצוע אבן הדרך הרביעית.

(ג) **פרק ג' – SMART on FHIR**

(1) **חלוקת התמיכה – 40% מהתמיכה יחולק עבור תשתית SMART on FHIR** (התממשקות לאפליקציות לשירות המטופלים והמטפלים);

(2) **הפעילות הנתמכת** –

(א) העמדת תשתית טכנולוגית התומכת ב-SMART on FHIR, ובכלל משאבי ה-FHIR, כפי שאושרו בתכנית העבודה;

(ב) הטמעת אפליקציות בקופה לשירות מטופלים ומטפלים בסטנדרט FHIR;

(3) **תנאים לפעילות הנתמכת** –

(א) הקופה מאפשרת הנגשת מידע רפואי בסטנדרט SMART on FHIR לאפליקציות הנותנות שירות לכלל מבוטחי הקופה הרלוונטיים, ואשר אושרו על ידי הקופה לשימוש עבור מבוטחי הקופה;

(ב) האפליקציה מוטמעת בקופה בהתאם לארכיטקטורה שאושרה בתכנית העבודה;

(ג) הארכיטקטורה כוללת שירות המאפשר לוודא את קבלת הסכמת המטופל לשיתוף המידע, וניהול מתן הרשאות על ידי המטופל בהתאם לדרישות המשרד;

(ד) 10% ממבוטחי הקופה או מהצוות המטפל בקופה המהווים קהל יעד אפשרי לאותה אפליקציה הינם משתמשים פעילים, כפי שיאושר על ידי המשרד;

(ה) לא נחתם הסכם בלעדיות בין מפתח האפליקציה לקופה;

(4) **אופן החלוקה** –

(א) עבור האפליקציה הראשונה המיועדת למטופלים, שהוטמעה בקופה ושעומדת בתנאים המפורטים בפרק זה, תהיה הקופה זכאית לסכום של 17% מהסכום העומד לחלוקה בפרק זה;

(ב) עבור כל אפליקציה נוספת המיועדת למטופלים או למטפלים – 4% מהסכום העומד לחלוקה בפרק זה, ובלבד שהקופה הייתה זכאית לקבל תמיכה כמפורט בפסקת משנה (א);

(ג) זכאות הקופה לתמיכה תחושב אחת לרבעון, בהתאם לחלקה היחסי בזכאות שצברה מתוך כלל הזכאויות שצברו קופות החולים לפי פסקאות משנה (א) ו-(ב);

(ד) על אף האמור בפסקאות משנה (א)-(ג), רשאית ועדת התמיכות להפחית סכום אחיד מהסכום שיוענק עבור כל אפליקציה;

(ה) סכום התמיכה הכולל עבור קופה אחת לפי פרק זה לא יעלה על 37% מהסכום העומד לחלוקה בפרק זה;

(5) **אבני דרך** – סכום התמיכה לו זכאית הקופה יחושב אחת לרבעון עד לסוף תוקפם של מבחנים אלה או עד גמר התקציב המיועד לפרק זה (המוקדם מבניהם); למען הסר ספק, ניתן לשלם בהתאם לפרק זה גם בטרם ביצוע אבני הדרך ארבע וחמש בפרק ב'.

7. נהלים

(א) התמיכה במסגרת מבחנים אלה תיעשה בכפוף להוצאות ובעבור סכום התמיכה במבחנים אלה; על קופת החולים להעמיד כספים למימון עצמי בשווי של לא פחות מ-40% מעלות הפעילות הנתמכת.

(ב) במסגרת הבקשה לתמיכה בעד תחום הפעילות הנתמכת לפי מבחנים אלה, לא תבקש קופת חולים תמיכה בעד הוצאות שהוצאו במסגרת תחום פעילות אחר.

(ג) לא תינתן תמיכה לקופת חולים שאינה משתפת פעולה עם ביקורת מטעם המשרד, לרבות הצגת אסמכתאות על הוצאות בפועל על פי דרישה.

(ד) בלי לגרוע מן האמור לעיל, קופת חולים שעשתה שימוש בלתי נאות בכספי התמיכה, היינו השתמשה בהם שלא בעד הפעילות הנתמכת במבחנים אלה, שימשה כעמותת צינור לשם העברת הכספים לגוף אחר, או הגישה דיווחים כוזבים לגבי כספי התמיכה שאושרו לה, תידרש להשיב את סכום התמיכה שניתן לה ותישלל אפשרותה לקבל תמיכה מן המשרד בשנתיים שלאחר מכן.

(ה) קבלת התמיכה לפי מבחנים אלה מותנית בדיווח של קופת החולים על עמידה בתנאי מבחנים אלה, כפי שיורה המשרד, לרבות הוצאה בפועל בגין רכש השירותים; קופות החולים יציגו למשרד אסמכתאות לעמידה באבני דרך בכל אחד מן השלבים המפורטים במבחנים; האסמכתאות יוגשו למשרד חתומות ומאושרות בידי קופת החולים בצירוף חתימת מנהל הכספים, בטרם קבלת כספי התמיכה.

(ו) קופת חולים לא תיתמך בעד פעילות שלא פורטה במסגרת התכנית.

8. תחילה ותוקף

תחילתם של מבחנים אלה ביום כ״ו בחשוון התשפ״ב (1 בנובמבר 2021), והם יעמדו בתוקפם עד יום י״ט בטבת התשפ״ד (31 בדצמבר 2023).

_____ התשפ״ב
(_____2021)

_____
ניצן הורוביץ
שר הבריאות

(803-35-2021-000154)

תוספת

נספח אבטחת מידע

1. כללי

תיושם אבטחת מידע כפי שהיא מוגדרת בתקן ISO-27799 ו-ISO-27001, אשר כוללת: שמירה על סודיות, שלמות ואמינות, זמינות ושרידות המידע; יישום זה יעשה במערכות המידע הרפואיות הממוחשבות בבתי החולים, במרפאות הקהילה ובחטיבת המרכזים הרפואיים; כל זאת בכפוף לתקנות הגנת הפרטיות ולחוקי אבטחת מידע.

2. עקרונות

במסגרת אבטחת המידע, יש לשים דגש על העקרונות הבאים –

(א) **תשתיות טכנולוגיית המידע** כדוגמת מערכות הפעלה בשרתים, בסיסי נתונים, תשתיות תוכנה יישומיות מרכזיות, רכיבי תקשורת יוגדרו אבטחתית בהתבסס על ״**נוהל תשתיות תקשוב מאובטחות במב״ר**״.

(ב) **פיתוח** – שילוב אבטחת מידע בכל רכש, פיתוח או שידרוג מערכות טכנולוגיית מידע, יתבסס על הדרישות לפיתוח מאובטח המנוסחות ב- ״**נוהל פיתוח מערכות מידע מאובטח במב״ר**״.

(ג) רשימת הכלים והטכנולוגיות המאושרים לשימוש תתעדכן מפעם לפעם כפי המופיע ב-״**תקנים וטכנולוגיות אבטחת מידע בתוקף**״.

(ד) ייעשה שימוש במגוון שיטות וכלים טכנולוגיים להבטחת שלמות ואמינות הנתונים המועברים בין רכיביה השונים של כל מערכת, בין אם מדובר במערכות בתוך הארגון (ממשק פנימי) ובין אם מדובר במערכות מהארגון החוצה (ממשק חיצוני).

(ה) **הזדהות** – יש ליישם חובת הזדהות חד ערכית על ידי משתמש למערכות טכנולוגיית המידע או לחילופין יש ליישם יכולת זיהוי חד ערכית לכל פעילות במערכת המבוצעת על ידי משתמש במערכת.

(ו) **הרשאות** – יש לוודא כי הענקת זכויות פעילות במערכות טכנולוגיית המידע תבוצע על בסיס ה״צורך לדעת״ ובמסגרתה –

(1) תהיה יכולת בקרה ניהולית בארגון, כגון קביעת הרשאות בהתאם לתפקיד בארגון או בהתאם לתפקיד המבוצע באותה עת;

(2) כל שינוי, הקפאה או ביטול של זכויות פעילות במערכות טכנולוגיית המידע והרשאות גישה, יבוצע בהתאמה ללוח הזמנים הרלוונטי לסטטוס העובד או המשתמש בארגון (דהיינו, בצמוד למעבר תפקיד, יציאה לחופשה ארוכה, ובסיום העסקה);

(3) נדרשת ביקורת תקופתית על פרטי רישום המשתמשים, לכל מערכות המידע, לשם ווידוא שלמותם, דיוקם וכי הגישה עדיין נדרשת.

(ז) **הצפנת תווך** – יש להצפין את התקשורת בתווך שבין כל רכיבי המערכת; ההצפנה תעשה בחוזק AES 256 ובהתאם לשימוש בפרוטוקול TLS1.2.

(ח) **הצפנת מידע במנוחה** –יש להצפין מידע רגיש כגון סיסמאות.

(ט) **חתימה** – המערכת תתמוך בחתימות תוך שימוש באלגוריתם SHA256 ובמפתח 2036 ביט; עם יכולת עתידית להתאמה לדרישות של אורך מפתח חתימה 4096 ביט ואלגוריתמי גיבוב מתקדמים אף יותר.

(י) **אירועי אבטחת מידע** – במערכות טכנולוגיית המידע ישולבו אמצעים לגילוי, מניעה, תיעוד, התאוששות והגנה מפני קוד זדוני בתחנות הקצה, בשרתים ובשערי הארגון או על פי ארכיטקטורה מתאימה בהתאם להחלטת הארגון; כמו כן יש להגדיר נוהל טיפול במקרה של כשל אבטחתי במערכות.

(יא) **גיבוי** – יוכנו עותקי גיבוי של מידע ושל תוכנות והם ייבדקו באופן סדיר, לפי מדיניות הגיבוי המוסכמת.

(יב) **העברת מידע אישי** – העברת מידע אישי תיעשה בכפוף לדרישות בחוק ובתקנות להגנת הפרטיות ולהנחיות הרשות להגנת הפרטיות, ובפרט, הצפנת תווך או מידע בעת העברתו בתווך ציבורי.

3. בקרות

(א) הספק יטמיע מנגנון נתיב בקרה לניטור ומעקב אחר ביצוע פעולות ושאילתות במערכת, ובנוסף, או לחלופין, בחומרה (לרבות פעולות שמתבצעות על ידי המערכת, על מנת לאפשר למשרד הבריאות לקיים ניטור כאמור.

(ב) על קובץ התיעוד של נתיב הבקרה (Log) (להלן: **קובץ התיעוד**) להכיל את הנתונים הרלוונטיים, כך שיתאפשר לגלות ניסיונות גישה ופעולות לא מורשות ולזהות את מקורן; נתיב הבקרה יכלול, לכל הפחות, מידע על מהות הפעולה, מקור הגישה וזמן הגישה.

(ג) 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 ואת רכיב טכנולוגיית המידע שבו נעשה שימוש.

(ד) פרק הזמן לשמירת קובץ התיעוד ייקבע על ידי המשרד.

(ה) כל ניסיון גישה כושל וחריג לחומרה, למערכת, ולמערכות ברשת אליו ניגשים המערכת והחומרה, ינוטר ויתועד במנגנון אירועים.

(ו) על הספק לוודא כי שעון מנגנון הניטור יהיה מסונכרן עם מקור שעון מדויק לצורך דיוק התיעוד.

(ז) קובץ התיעוד יאובטח בפני מחיקה, שינוי או קריאה בלתי מורשים, ובכלל זה –

(1) רישום אירועים כגון אירועי ניהול מפתחות;

(2) חיתום משתמשים;

(3) אתחול וכיבוי;

(4) יצירת התראות כדוגמת עבודה מחוץ לשעות מוגדרות, ריבוי חתימות וקצב גבוהה;

(5) שינוי פרמטרי Audit;

(6) יצירת התראות כדוגמת עבודה מחוץ לשעות מוגדרות, ריבוי חתימות וקצב.

(ח) שיח לא פעיל יופסק לאחר פרק זמן מוגדר של אי פעילות שיותאם למיקום תחנת העבודה ולפעילות המתבצעת באמצעותה.

(ט) ככל שהדבר רלוונטי, מעגל הגנה ראשון לרכיבי טכנולוגיית המידע יהיה מעגל אבטחה פיזי.

4. ניטור

(א) הספק יידרש לבצע ניטור למערכת שיכלול –

(1) ניטור לוגים – איתור בזמן אמת, או בדיעבד, של בעיות טכניות;

(2) ניטור ביצועים – מעקב אחר עומסים;

(3) ניטור ומעקב אחר פעילויות חריגות או עויינות (ניסיונות הזדהות כושלים, גישה לא מורשית, ניסיונות כניסה כפולים ועוד).

(ב) באחריות הספק לוודא כי אחת ל-12 חודשים לפחות, לאורך תקופת ההתקשרות, יתבצעו מבדקי אבטחת מידע תקופתיים מסוג Penetration tests ו–Vulnerability scan הכוללים בין השאר:

(1) בדיקות לתשתיות שתסופקנה על ידי החטיבה;

(2) בדיקות של מערכת הניהול;

(3) בדיקות Social engineering או הדרכות מודעות לעובדים.

(ג) באחריות הספק לזהות אירועי אבטחת מידע בשירות, להתריע לחטיבה מידית, ולא יאוחר מ-48 שעות מרגע גילוי אירוע האבטחה, ולפעול לטיפול באירוע תוך שמירה על הסטנדרטים המקובלים בשוק ועל חוקי מדינת ישראל.

(ד) הספק מתחייב כי אירועי אבטחת מידע ידווחו לחטיבה עם זיהוים, לרבות העברת דיווח לתשתיות הניטור וההגנה (Siem) של החטיבה; אירועים שיוגדרו ברמת סיכון גבוה, כגון חשד לנגישות זרה והזלגת מידע – ידווחו מידית.

(ה) כחלק מתהליך ניהול אירוע, הספק מתחייב לשמור את כל המידע הרלוונטי כולל קבצי לוג, פעולות שבוצעו במערכת, תרחישי תגובה ומצבי פלטפורמה.