ט' אדר, תשפ"א
21 פברואר, 2021
מס': 2/2021

<u>הנדון: שימוש במחשוב ענן במערכת הבריאות</u>

1. <u>רקע</u>

בשנים האחרונות גוברת בעולם מגמת המעבר לשימוש בשירותי ענן בתעשיות רבות. טכנולוגיית הענן היא מרכיב חשוב בהכנסת חדשנות לארגון. היא מאפשרת לארגון גמישות תפעולית ואת היכולת לנצל באופן יעיל ומיטבי את משאבי המחשוב העומדים לרשותו, לצד חיסכון בעלויות הפעלת אותם שירותים בתוך הארגון. בנוסף, טכנולוגיית הענן יכולה לסייע לארגוני בריאות לפתח יכולות תפעוליות ומחקריות מתקדמות, וכן להטמיע פתרונות חדשניים, אשר רבים מהם פועלים כיום בענן בלבד.

הפעלת יישומים באמצעות מחשוב ענן צריכה להיעשות באופן מושכל ומאוזן. בהתאם, האסדרה הנוכחית מבקשת לאפשר לארגוני הבריאות לעשות שימוש בכלים ובאמצעים, אשר ביישום נכון, יכולים לסייע להם לעשות שימוש בטכנולוגיות מתקדמות ופיתוחים חדשניים לצד עמידה בדרישות הציות החלות עליהם לפי הוראות חוק הגנת הפרטיות ותקני אבטחת המידע והגנת הסייבר ולהתמודד עם סיכוני אבטחת מידע, פרטיות, ושמירה על הרציפות התפעולית של הארגון.

משרד הבריאות רואה חשיבות רבה בהרחבת השימוש במחשוב ענן על ידי ארגוני הבריאות ככלי להתמודדות עם האתגרים התשתיתיים, הארגוניים, הטכנולוגיים והכלכליים הניצבים בפניהם, ומעודד את חיזוק היכולות הטכנולוגיות של ארגוני הבריאות כמרכיב חשוב בקידום תחום הבריאות הדיגיטלית, וכדי ליישר קו אל מול גופים ומערכות מקבילות בעולם.

בהחלטת ממשלה מס' 2443 מיום 15.2.2015 בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" הונחו המנהלים הכלליים של משרדי הממשלה ויחידות הסמך לפעול לשיפור רמת הגנת הסייבר בתחומי משרדם. מתוקף החלטת הממשלה מונה במשרד הבריאות ממונה הגנת סייבר. בהמשך לכך, הוקמה במשרד הבריאות יחידת סייבר אשר אמונה על הנחיית ארגוני הבריאות בישראל בכל הנוגע לאבטחת מידע והגנת סייבר, ובכלל זה ליישומם בעת השימוש במחשוב ענן.

2. <u>מטרה</u>

קביעת אמות מידה להפעלה נאותה של יישומי מחשוב באמצעות מחשוב ענן על ידי ארגוני בריאות כדי לעודד כניסת טכנולוגיות מתקדמות לשימוש על ידי ארגוני הבריאות.

3. <u>הגדרות</u>

3.1. "**ארגון בריאות**" – מרפאה, קופת חולים או בית חולים;

3.2. "**ועדת ענן ארגונית**" – ועדה הפועלת בארגון הבריאות וכוללת לפחות את בעלי התפקידים הבאים: נציג המנהל הכללי; נציג היועץ המשפטי של הארגון; ממונה אבטחת המידע והגנת הסייבר של הארגון או נציגו; ממונה הגנת הפרטיות של הארגון או נציגו, ככל שמונה; ומנהל מערכות המידע של הארגון או נציגו. ארגון בריאות יכול להגדיר ועדה קיימת כוועדת הענן הארגונית, ובלבד שהיא עומדת בתנאים הקבועים בהוראות אלו. חבר ועדה יכול להיות בעל תפקיד אחד או יותר, בהתאם להגדרות תפקידיו המקצועיים בארגון, ובלבד שהוועדה כוללת לפחות שלושה חברים.

3.3. "**ועדת ענן מגזרית**" – ועדה הפועלת במשרד הבריאות בה יהיו חברים: נציג מנכ"ל משרד הבריאות; נציג היועץ המשפטי של משרד הבריאות; ממונה אבטחת המידע והגנת הסייבר במשרד הבריאות; נציג אגף בריאות דיגיטלית במשרד הבריאות; נציג מערך הסייבר הממשלתי; נציג רשות התקשוב; ונציג הרשות להגנת הפרטיות;

3.4. "**מחשוב ענן**" – תשתיות ומשאבי מחשוב (כדוגמת שרתים, אמצעי אחסון, רשתות, יישומים ושירותים), אשר הגישה אליהם נעשית באמצעות רשת האינטרנט ו/או קו תקשורת ייעודי, לפי דרישה ולפי שימוש;

3.5. "**ספק מחשוב ענן**" – חברה מסחרית אשר מספקת שירותי מחשוב ענן (Vendor) או שירותי תשתיות ענן (Provider) לארגון הבריאות;

4. <u>מדיניות ענן ארגונית</u>

4.1. ועדת הענן הארגונית תגבש מדיניות ענן ארגונית בהתאם להוראות אלו, כתנאי להפעלת וועדת ענן ארגונית. מדיניות הענן תובא לאישור הנהלת ארגון הבריאות.

4.2. מדיניות הענן הארגונית תכלול התייחסות, לכל הפחות, לנושאים הבאים:

4.2.1. הקווים המנחים ואמות המידה לקביעת סוגי היישומים שניתן לעשות בהם שימוש במחשוב ענן;

4.2.2. ההליכים הארגוניים ומדרג הסמכויות הארגוני לאישור שימוש במחשוב ענן, לרבות מתודולוגית ניהול הסיכונים של הארגון;

4.2.3. סמכויות ואחריות בעלי התפקידים השונים בכל הנוגע לשימוש במחשוב ענן, לרבות, תחזוקה, ניטור ואבטחת מידע והגנה בסייבר;

4.2.4. עקרונות התקשרות עם ספק מחשוב ענן, לרבות האמצעים והמנגנונים לפיקוח ולבקרה על ספקים;

4.2.5. מדיניות אבטחת המידע, הגנת הסייבר והגנת הפרטיות של הארגון, בכל הנוגע לשימוש במחשוב ענן, לרבות הבקרות שייושמו על ידי הארגון;

4.2.6. מחזור החיים של תהליכי השימוש במחשוב ענן, לרבות הפסקת השימוש בו;

4.2.7. סוגיות רלוונטיות נוספות לאור מאפייני ארגון הבריאות.

4.3. ועדת הענן הארגונית תקיים אחת לשנה דיון על יישום מדיניות הענן הארגונית, כולל בחינה של הצורך בעדכון המדיניות בהתאם להתפתחויות הטכנולוגיות ולשינויים רגולטוריים, ארגוניים ועסקיים בשנה החולפת.

4.4. הנהלת ארגון הבריאות תקיים דיון על מדיניות הענן הארגונית בכל עת שיבוצע שינוי או עדכון מהותי של המדיניות, אך לא פחות מאחת לשנתיים.

4.5. באחריות ארגון הבריאות להעביר לידיעת ממונה אבטחת מידע והגנת הסייבר במשרד הבריאות את מסמך מדיניות הענן הארגונית עם אישורה בארגון בפעם הראשונה כמו גם לאחר כל עדכון או שינוי מהותי.

5. <u>הפעלת יישום במחשוב ענן</u>

5.1. ארגון בריאות רשאי להפעיל יישום במחשוב ענן בהתאם להוראות אלו.

5.2. המנהל הכללי של ארגון הבריאות ימנה את חברי וועדת הענן הארגונית בהתאם להנחיות חוזר זה ומדיניות הענן הארגונית. באחריות ארגון הבריאות להעביר לידיעת ממונה אבטחת מידע והגנת הסייבר במשרד הבריאות את כתבי המינוי של חברי הוועדה הארגונית קודם לתחילת פעילות הוועדה ולאחר כל שינוי בהרכב חבריה.

5.3. בעת הפעלת יישום מחשוב ענן יש להבטיח כי לארגון הבריאות בעלות מלאה על המידע המועבר, כמו גם יכולת להגביל את אופן השימוש בו.

5.4. הפעלת יישום במחשוב ענן תתאפשר **<u>רק</u>** לאחר שבוצע הליך פנים ארגוני לבחינה של המעבר לשימוש במחשוב ענן. הליך הבחינה יתייחס לכל הפחות להיבטים הבאים:

5.4.1. התהליך העסקי במסגרתו נעשה שימוש במערכת או במידע שמבוקש להעבירם לענן, ובכלל זה החשיבות והתועלות עבור הארגון או המטופלים במעבר למחשוב ענן;

5.4.2. ניתוח המידע והמערכת, לרבות מיפוי וסיווג המידע, המשתמשים וספק הענן המבוקש;

5.4.3. תאימות השימוש במחשוב ענן על פי כל דין, ובפרט מול חוק הגנת הפרטיות והנחיות המשרד בנושאים אלו;

5.4.4. הערכה וניהול של הסיכונים מהשימוש במחשוב הענן בהתאם למדיניות הארגונית כפי שאושרה בהתאם לאמור בסעיף 4.2 לעיל ועל פי העקרונות המפורטים בנספח א';

5.4.5. הארכיטקטורה, הממשקים ודרישות אבטחת המידע והגנת הסייבר;

5.4.6. הצגת בקרות מפצות מול תהליך ניהול הסיכונים.

5.5. בהתאם לממצאי תהליך הערכת הסיכונים כמפורט בסעיף 5.4.4 לעיל, יקבע הסיווג של רמת הסיכון בהפעלת היישום במחשוב ענן. קביעת רמת הסיווג כאמור, תאושר על ידי ממונה אבטחת המידע והגנת הסייבר של הארגון, היועץ המשפטי וממונה הגנת הפרטיות בארגון או נציגיהם.

5.5.1. באם תוצאות הערכת הסיכונים הראתה כי רמת הסיכון בהפעלת היישום במחשוב הענן היא נמוכה או בינונית, הגורם המאשר את הפעלת היישום במחשוב ענן יהיה ועדת הענן הארגונית.

5.5.2. באם תוצאות הערכת הסיכונים הראתה כי רמת הסיכון בהפעלת היישום במחשוב הענן היא גבוהה, הגורם המאשר את הפעלת היישום יהיה ועדת הענן הארגונית, ובלבד שהתקבלה חוות הדעת של ועדת הענן המגזרית בנוגע להפעלת היישום כאמור.

5.6. ועדת הענן המגזרית מוסמכת לקבוע את הבאים:

5.6.1. הפעלה של יישום מסוים במחשוב ענן ברמת סיכון גבוהה תאושר על ידי ועדת הענן הארגונית בלבד. ועדת הענן המגזרית רשאית לקבוע תנאים לעניין זה;

5.6.2. ועדת ענן ארגונית מסוימת לא תידרש לחוות דעת ועדת הענן המגזרית לצורך אישור הפעלה של יישומים ברמת סיכון גבוהה. ועדת הענן המגזרית רשאית לקבוע תנאים לעניין זה;

5.6.3. ועדת ענן ארגונית מסוימת תידרש לחוות דעתה של ועדת הענן המגזרית לצורך אישור הפעלה של יישומים שנמצאו כבעלי סיכון נמוך או בינוני.

5.7. אישור ועדת הענן ידרש בעת ההפעלה הראשונה של היישום במחשוב ענן וכן בכל שינוי מהותי באופן ההפעלה האמור, לרבות בארכיטקטורה, בתשתית ובטכנולוגיה שבה נעשה שימוש.

6. <u>התקשרות עם ספק מחשוב ענן</u>

6.1. ארגון בריאות לא יעשה שימוש במחשוב ענן אלא אם נחתם הסכם התקשרות בינו לבין ספק מחשוב הענן, וכל עוד ההסכם כאמור בתוקף.

6.2. לפני ההתקשרות של ארגון הבריאות עם ספק מחשוב הענן, על ארגון הבריאות לבצע בחינה והערכה של יכולתו של ספק מחשוב הענן לספק את השירותים המבוקשים, בהתייחס, בין היתר, לנושאים הבאים ובהתאם למודל השימוש במחשוב ענן:

6.2.1. כשירותו המקצועית והיכולות הטכנולוגיות שלו לספק את השירותים המבוקשים ולעמוד בהתחייבותיו לפי ההסכם;

6.2.2. אמצעי אבטחת המידע, הגנת הסייבר והגנת הפרטיות המיושמים על ידו;

6.2.3. האמצעים הכלכליים ויכולתו הפיננסית לעמוד בהתחייבויותיו כלפי ארגון הבריאות;

6.2.4. האמצעים שמעמיד ספק מחשוב הענן לארגון הבריאות כדי לאפשר לארגון הבריאות לעמוד בדרישות הדין הישראלי וההנחיות הרגולטוריות החלות עליו בכל הנוגע לשימוש במחשוב הענן;

6.2.5. ההשלכות הנובעות משימוש במחשוב ענן הנמצא מחוץ לגבולות מדינת ישראל, לרבות תחולת דין זר על המידע במקרה זה;

6.3. הסכם ההתקשרות בין ארגון הבריאות לספק מחשוב הענן יכלול, לכל הפחות, התייחסות לנושאים הבאים:

6.3.1. חלוקת האחריות בין ארגון הבריאות לספק מחשוב הענן בהתאם לסוג השירות ולמודל השימוש במחשוב ענן שהוא מספק;

6.3.2. מנגנוני ואמצעי אבטחת המידע, הגנת הסייבר והגנת הפרטיות שייושמו על ידי כל אחד מהצדדים בהתאם לחלוקת האחריות ביניהם ולמודל השימוש במחשוב ענן;

6.3.3. האמצעים שיועמדו לרשות ארגון הבריאות לביצוע בקרות על השימוש במחשוב ענן ועל ספק מחשוב הענן, לרבות על ספקי משנה שלו ו/או צדדים שלישיים מטעמו ועל פעילותם, ו/או לקבלת מידע על מבדקים וביקורות בנושאים האמורים;

6.3.4. ההסדרים שיופעלו על ידי ספק מחשוב הענן להתמודדות ולטיפול באירוע סייבר או אירוע חירום, לרבות אופן ותדירות הדיווחים הנמסרים לארגון הבריאות על אירועים אלו;

6.3.5. תקופת ההתקשרות, הסדרים להפסקת ההתקשרות וליישוב מחלוקות ולהעברת המידע לספק מחשוב ענן אחר, והוראות לעניין אופן החזרת המידע לארגון הבריאות או מחיקתו באופן המלא והמקיף ביותר האפשרי בתום תקופת ההתקשרות;

6.3.6. מנגנון ההמשכיות העסקית של ספק מחשוב הענן;

6.4. ארגון הבריאות יבצע בחינה והערכה מחודשת של ספק מחשוב הענן ושל שירותי מחשוב הענן המסופקים על ידו מעת לעת בהתאם לשינויים טכנולוגיים, רגולטוריים, ארגוניים ועסקיים, אך לא פחות מאחת לשנתיים.

6.5. ככלל, ניתן לעשות שימוש במחשוב ענן הנמצא במדינה שעומדת בדרישות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001.

7. ניטור ובקרה

7.1. על ארגון הבריאות לנטר ולבצע פעולות פיקוח ובקרה על השימוש במחשוב ענן, בהתאם לעקרונות שהותוו במדיניות הענן הארגונית, ממצאי ניהול הסיכונים והבקרות שהוגדרו בעת אישורו, והנחיות משרד הבריאות.

8. תיעוד, דיווח ושמירת מסמכים

8.1. ארגון הבריאות יתעד את תהליכי האישור לשימוש במחשוב ענן, על כל שלביהם, לרבות התייחסות כלל הגורמים הרלוונטיים (ככל שנדרשת), והחלטות שהתקבלו. התיעוד יישמר לתקופה שלא תפחת מ-7 שנים מתום תקופת השימוש במחשוב ענן.

8.2. ארגון בריאות ידווח לממונה אבטחת המידע והגנת הסייבר במשרד הבריאות באופן שוטף על כל שימוש חדש במחשוב ענן שאושר על ידי הארגון, בצירוף מסמכי האישור ופרוטוקול ועדת הענן הארגונית, בתוך 30 ימים ממועד חתימה על הסכם התקשרות עם הספק.

8.3. ארגון הבריאות ידווח אחת לשנה על כל השימושים במחשוב ענן שהפעלתם הופסקה בשנה הקודמת למועד הדיווח, וככל שסיבת הפסקת השימוש נובעת מהיבטי אבטחת מידע ו/או הגנת הפרטיות ידווחו גם הנימוקים לכך.

8.4. משרד הבריאות רשאי, לפי שיקול דעתו, לדרוש קבלת נתונים ומסמכים נוספים בנוגע לכל שימוש במחשוב ענן שאושר או שהופסקה הפעלתו.

9. כללי

9.1. ארגון הבריאות רשאי להסתייע ביועצים חיצוניים בעלי מומחיות מוכרת וניסיון מוכח בתחום מחשוב הענן כדי לעמוד בדרישות אלו.

9.2. הוראות חוזר זה יחולו גם על הסדרת השימוש במחשוב ענן לצורך ביצוע מחקרים במידע בריאות לפי חוזר מנכ"ל 1/2018 (ו/או כל חוזר אחר שיבוא במקומו), שבהם ניתנת גישה למידע בריאות בסביבה מאובטחת המנוהלת על ידי ארגון הבריאות.

9.3. יש לפעול על פי ההנחיות הטכניות במפורטות בנספח ב' במסמך זה. כן יש להסתייע בהנחיות ובמסמכים מקצועיים המפורסמים מעת לעת על ידי משרד הבריאות, רשות התקשוב, יה"ב ומערך הסייבר הלאומי בנוגע לשימוש במחשוב ענן, ככל שהן חלות על ארגון הבריאות.

9.4. הוראות אלו אינן גורעות מהחובות החלות על ארגוני בריאות על פי חוק הגנת הפרטיות, התשמ"א-1981 והתקנות מכוחו, לרבות בכל הנוגע למיקור חוץ.

9.5. שימוש במחשוב ענן לא יגרע מאחריותו של ארגון הבריאות לשמור על שלמות, זמינות וסודיות המידע, וליישם את דרישות אבטחת המידע והגנת הפרטיות החלות עליו כבעלים ו/או כמחזיק במידע על פי כל דין.

9.6. דיווחים על פי חוזר זה יש להעביר לכתובת המייל infosec@moh.gov.il.

10. אחריות ליישום

מנהל ארגון הבריאות אחראי על יישום הוראות אלו בארגונו.

11. בקרה

ביצוע הנחיות אלו ייבדק כחלק מהבקרות השוטפות שעורך משרד הבריאות בארגוני בריאות.

12. <u>תחולה</u>

12.1. ארגון בריאות יפעל על פי הוראות חוזר זה, לכל המאוחר, בתוך 6 חודשים ממועד פרסומו.

12.2. על אף האמור בסעיף 12.1 שלעיל, הוראות החוזר ייכנסו לתוקף לגבי מחשוב ענן שהשימוש בו החל ערב פרסום חוזר זה, במועד בו תחודש ההתקשרות של ארגון הבריאות עם ספק מחשוב הענן או בתום שנתיים ממועד כניסת הוראות אלו לתוקף, לפי המוקדם.

בכבוד רב,

פרופ' חזי לוי

העתק: ח"כ יולי אדלשטיין, שר הבריאות
247651821

נספח א' – תהליך בחינת ניהול סיכונים להפעלת יישום במחשוב ענן במערכת הבריאות

תהליך הבחינה של המעבר לשימוש במחשוב ענן יכלול, לכל הפחות, התייחסות להיבטים המפורטים להלן.[1]

1. <u>תיאור התהליך העסקי</u>

1.1. יש לפרט את התהליך העסקי שבמסגרתו ייעשה שימוש ביישום שמבוקש להעבירו למחשוב ענן, וכן את קשרי הגומלין לתהליכים בתוך הארגון ולמערכות משיקות בענן או בארגון הבריאות.

1.2. יש לפרט את ייעוד היישום ואת מטרות השימוש בו, וכן הסיבות והתועלות הצפויות מהמעבר לשימוש במחשוב ענן.

2. <u>ניתוח המידע והיישומים</u>

יש לבצע הליך בחינה וניתוח מלא של כלל המידע והיישומים אשר מיועדים לעבור למחשוב ענן, ובתוך כך יש לבחון את הבאים:

2.1 **מיפוי המידע**. יש למפות את המידע שצפוי לעבור לסביבת הענן, ובכלל זה האם הוא פורסם לציבור, האם חשוף לגורמים חיצוניים, האם קיים סיווג ביטחוני למידע, האם הוא יכיל נתונים אישיים ופרטיים, האם יכיל נתונים המשפיעים על התפקוד התקין של הארגון ועשויים לפגוע במשילות, האם יכיל נתונים רפואיים, האם המידע מזוהה ובאיזה מידה ועוד.

2.2 **סיווג המידע.** יש לבחון את רגישות המידע, בין היתר, לפי נוהל סיווג מידע של מגזר הבריאות (א.8), כפי שיהיה בתוקף.

2.3 **היקף המידע.** יש לבחון את כמות המידע הצפוייה להיות מועברת במסגרת השימוש במערכת.

3. <u>ניתוח המערכת</u>

3.1. **מיפוי הממשקים**. יש לבחון את הממשקים החיצוניים לרשת הפנימית ואת הממשקים החיצוניים לספקים אחרים. כך, יש להתייחס לתדירות הקישור לממשק, כיוון הממשק, פרוטוקול, סוג ההזדהות ואופי הקריאה, וכן את בקרות אבטחת מידע שיינתנו ליישום.

3.2. **משתמשים**. יש למפות ולהגדיר את הגורמים שעושים שימוש ביישום ואת ההרשאות הנדרשות מהם ואת הגורמים שיהיו בעלי גישה למחשוב הענן. יש להתייחס לסיווג המשתמשים, כמות המשתמשים, מנהלי המערכת, הגדרת המשתמשים והרשאות ואופן הגישה אל היישום.

3.3. **תשתיות הארגון הקיימות**. יש לפרט ולבחון את המערכות או סביבות הענן הקיימות בארגון; התממשקות אפשרית של היישום למערכות אחרון בארגון; וניסיון העבר מול העברת מערכות למחשוב ענן בארגון.

3.4. **ספק התקשורת אל/ממחשוב הענן**. יש לבחון - מי הספק? מה התשתיות שלו? מה הרגולציות שחלות עליו ועל התשתיות? מה רמת השירות המוגדרת? אילו אמצעי הגנה פנימיים וחיצוניים הספק מאפשר? מי יהיו בעלי גישה למחשוב הענן? ומה הוא מודל השירות המבוקש.

3.5. **מאפייני השירות המבוקש ואופן היישום**. יש לבחון את התשתיות הקיימות של הספק והארגון ביחס להפעלת היישום המבוקש, כמו גם את אפשרויות הגיבוי, שרידות וניטור המידע והיישום. זאת, בנוסף לאופן שמירה והצפנת הנתונים, תהליכי מיגרציה בסיום התהליך וביצוע מבחני חדירות באם רלוונטי.

[1] משרד הבריאות פיתח בשיתוף עם מערך הסייבר, הרשות להגנת הפרטיות ורשות התקשוב כלי עזר לניהול סיכונים, במטרה לסייע לארגוני הבריאות בביצוע ניהול הסיכונים לפי דרישות חוזר זה. ארגון בריאות רשאי לעשות שימוש בכלי ניהול הסיכונים כפי שהוא או להתאימו לצרכיו.

4. תאימות רגולטורית וחוקית

וידוא כי התהליכים הנדרשים עומדים בדרישות על פי דין ובהנחיות משרד הבריאות, מערך הסייבר ורשות התקשוב.

5. ניתוח הסיכונים

5.1. יש למפות את כלל הסיכונים האפשריים מהשימוש במחשוב ענן וביחס לניתוח סעיפים 1-4 לנספח זה. ככל שרלוונטי, יש להתייחס לסיכונים פרטניים הנובעים מהשימוש במידע רפואי ו/או מהיישום המיועד לעבור למחשוב ענן ו/או מהמאפיניים של ארגון הבריאות.

5.2. בעבור כל אחד מהסיכונים, יש להתייחס לסיכוי להתממשותו, לחומרת הפגיעה, כמו גם לבקרות שיופעלו על מנת לאזן ולהקטין את סיכויי ההתממשות ואת חומרת הפגיעה.

5.3. את הסיכונים יש לבחון על פי ערכי סודיות, זמינות ושלמות המידע ובהתאם למודל השימוש במחשוב ענן שנקבע ולחלוקת האחריות בין ספק מחשוב הענן וארגון הבריאות.

5.4. ככלל, רמת הסיכון תקבע בין היתר בהתחשב בפרמטרים הבאים: סוג המידע ורגישותו; היקף המידע המועבר למחשוב ענן – הן מבחינת מספר הרשומות והן מבחינת עומק המידע בכל רשומה; משך הזמן שהמידע יימצא בענן.

5.5. בעבור כל סיכון יש להגדיר את האמצעים אשר ייושמו על ידי הארגון/הספק על מנת לתת מענה לאותו סיכון, כמו גם את סיכוייהם למזער את הסיכון האמור.

6. ארכיטקטורה מוצעת

יש להציג את הארכיטקטורה המוצעת לפיתרון, ובכלל זה את רכיבי הפיתרון, הממשקים, מנגנוני האבטחה שיופעלו ואופן הטמעתם.

נספח ב' - הנחיות היחידה להגנת הסייבר במגזר הבריאות

דוגמאות לאיומים במעבר לענן ציבורי

להלן מספר דוגמאות לסיכונים ותרחישי איום אשר יש לשקול את השפעתם ודומיהם בעת גיבוש החלטה על מעבר לסביבות ענן ובחינת תהליכי הבקרה להפחתת הסיכון.[2] יובהר כי **מדובר בדוגמאות בלבד ולא ברשימה ממצה** של סיכונים ותרחישי איום, **ויש לבחון סיכונים ואיומים נוספים הרלוונטיים לשימוש בענן ציבורי, בהתאם לסוג השירות ומאפייניו וסוג המערכת והמידע המועברים לענן**.

1. חשיפה או זליגת מידע

איומי חשיפה או זליגת מידע בסביבות מחשוב ענן יכולים להיגרם כתוצאה ממספר תרחישים. להלן דוגמאות לתרחישים נפוצים:

1.1. חשיפת מידע כתוצאה מהפרדה לא יעילה בין לקוחות הענן (Tenants) החולקים את משאבי המחשוב.

1.2. חשיפת מידע עקב צו בית משפט של ממשלה זרה. שמירת מידע בתחום שיפוט שאינו מדינת ישראל חושף את המידע לחוקים ותקנות של הממשלות בהם פועל ספק הענן ומאחסן את המידע.

1.3. זליגת בסיסי נתונים ומידע רגיש אשר הועבר או הושאר בסביבת מחשוב הענן בסיום ההתקשרות עם ספק שירותי מחשוב ענן ללא בקרות מספקות אשר נדרשות בכדי להגן על מידע שכזה והותאמו למתאר האיומים הרלוונטיים ודרישות החוק להגנת הפרטיות בישראל.

1.4. חשיפת מידע ע"י עובדי ספק שירותי מחשוב הענן או צד שלישי בעל יכולת גישה למידע מחשוב ענן בדומה למיקור חוץ, מערב גורמים נוספים אשר אינם קשורים בקשר ישיר עם לקוח הענן ויתכן כי אינם מחויבים לחיסיון המידע ולבעליו.

1.5. חשיפת מידע עקב פריצה למכשיר קצה - מכשירי קצה רבים, לרוב מכשירים ניידים (Mobile Devices), עושים שימוש בשירותי מחשוב ענן לצורך שמירת המידע במיקום מרכזי ונגיש. פריצה למכשיר לאחר אובדן או גניבה שלו ובמקרה שהמכשיר אינו מוגן באמצעים הולמים, יכולה לגרום לחשיפת מידע.

2. אובדן או שבוש מידע

ספקי שירותי מחשוב הענן אינם חסינים לאובדן או שיבוש המידע כתוצאה מתקלה או מפריצה למערכת. ככלל, יש לבחון את האיום של אובדן מידע או שיבוש תחת התרחישים הבאים:

2.1. אובדן או שיבוש המידע כתוצאה מתקלה אצל ספק מחשוב הענן, לרבות הרס פיזי של תשתיות מחשוב.

2.2. אובדן או שיבוש המידע עקב התקפה שחדרה לסביבת מחשוב הענן. יש לזכור כי במחשוב ענן הניהול המרכזי והיכולת לשלוט במגוון רכיבים ממיקום יחיד מגדילים את היכולת לפגוע בכלל המידע והרכיבים.

2.3. ספק מחשוב הענן מפסיק את השירות.

2.4. יירוט התווך התקשורתי בין ספק מחשוב הענן לארגון הבריאות.

[2] מתוך הנחיית יה"ב מס' 5.5: "אבטחת מידע למעבר לענן ציבורי".

3. <u>אובדן זמינות המידע</u>

במחשוב ענן זמינות המידע תלויה במספר גורמים וישנם מספר תרחישים אשר יכולים לגרום לאובדן זמינות השירות. הערכת הסיכונים צריכה לכלול התייחסות לתרחישים אלו והשפעתם על הרציפות התפקודית של ארגון הבריאות:

3.1. ספק מחשוב הענן אינו יכול לאפשר זמינות למערכת כתוצאה מתקלה או התקפה למניעת שירות (DDOS).

3.2. לקוח השירות מאבד יכולת להתחבר למערכת כתוצאה מתקלה בחיבור לרשת או התקפה למניעת שירות.

3.3. חשבון הלקוח נחסם כתוצאה מתקלה, התקפה או הפרה של תנאי השירות.

3.4. ספק מחשוב הענן אינו עומד בעומסים או ב-SLA הנדרש למימוש המערכת של הלקוח.

3.5. ספק מחשוב הענן נאלץ להפסיק את השירות כתוצאה מצו בית משפט, הפרה של חוק/תקנות/החלטה עסקית/פיננסית.

3.6. לקוח השירות מאבד זמינות למידע בענן בשל אי הקצאת משאבים נכונה מראש מול ספק מחשוב הענן.

<u>בחירת ספק מחשוב הענן</u>

<u>מאפיינים לבחירת ספק מחשוב ענן ולהתקשרות החוזית עמו</u>

1. יש להעדיף בחירה של ספק מחשוב ענן המיישם תקינה בינלאומית מוכרת ומקובלת, כגון תקני ISO 27001, ISO 27017, ISO 27018, SOC 2, CSA, AICPA וכן בעל תאימות ל-GDPR;
2. יש להעדיף בחירה של ספק מחשוב ענן אשר מאפשר מספר אתרי זמינות בכל אתר גאוגרפי לצורכי זמינות ושרידות השירות.
3. יש לבחון את התחייבות ספק מחשוב הענן לזמינות האתרים הגאוגרפיים וקביעת מתן SLA מתאים בשלב התקשרות החוזה מולו עפ"י ערכי RPO ו-RTO של מערכות המידע בארגון, בהתאם למדיניות הענן הארגונית.
4. יש להעדיף בחירה של ספק מחשוב ענן המתחייב לקיום אפשרות חד-צדדית של הארגון להפסיק את השימוש בשירותי הספק או לעבור לספק אחר תוך העברת נתוניו הרלבנטיים ממערכות הספק תוך זמן קצר, מחיקתם ממערכות הספק והתחייבות הספק למחיקה באופן מלא ומקיף ביותר של המידע, מול תאימות לתקנים בינ-לאומיים מקובלים.

<u>עיצוב ארכיטקטורה מאובטחת לשירותי מחשוב הענן</u>

1. לאחר בחירת ספק מחשוב הענן, יש לבנות את ארכיטקטורת הפתרון למעבר לענן ע"י הארגון או ע"י ספק חיצוני מומחה בתחום מחשוב הענן ובליווי איש מקצוע שעבר הכשרה מתאימה בתחום מחשוב הענן, והוא בעל ניסיון ומומחיות בתחום ההגנה על תשתיות ענן.
2. ארכיטקטורת הפתרון צריכה להתייחס כבר בשלב הראשוני להיבטי אבטחת מידע והגנה בסייבר וליכולת למנוע מתרחישי האיום שנקבעו בסקר הסיכונים להתממש.
3. על הארגון לוודא כי עבור ארכיטקטורת הפתרון הכוללת ערוצים מ/אל ספק מחשוב הענן, קיימים אמצעים להגנת הסייבר ואבטחת המידע, שיאפשרו לצמצם, ככל שניתן, את השימוש בערוצים אלו לתקיפת הארגון ו/או לסיכון המידע.

4. על המידע של הארגון להיות מוצפן (לפחות בפרוטוקול 256AES) בעת העברתו בתקשורת וכן כאשר הוא מאוחסן במערכת שאינה לשימושו הבלעדי של הארגון (Multi-Tenancy). במקרים בהם יש קושי להצפין את כל המידע כאמור, יש להצפין לפחות את הנתונים שסווגו על ידי הארגון כרגישים ושיש בחשיפתם כדי לפגוע בארגון ובמטופליו. יש לבחון יישום המאפשר, ככל שניתן, לאחסן את מפתחות ההצפנה אצל הארגון.

5. בנוסף, יש לוודא יכולת לקיים הפרדה בין המתחמים שמחוץ לארגון הבריאות לבין אלו המקושרים לארגון ; וידוא זמינות השירות והמידע וחליפויות (BCP) בעת משבר תקשורת ; קיום ניהול משתמשים ומפתחות רלוונטיים כמו גם הגדרת הגורם התפעולי והרשאותיו השונות.

6. הארכיטקטורה צריכה להיות מאושרת ע"י מנהל אבטחת מידע ומנהל מערכות מידע.

<u>מעבר היישום לסביבת ייצור</u>

1. <u>בחינת אבטחת הפתרון המוצע</u>

טרם יישום הארכיטקטורה לסביבת הייצור יש לערוך בדיקת אבטחת מידע מקיפה לבחינת הפתרון המוצע. במסגרת התהליך, יש לבצע גם בדיקת עמידות וחוסן לפתרון המוצע, ולרכיבים שעליה מותקן היישום.

2. <u>מעבר היישום לסביבת ייצור</u>

2.1. טרם אישור היישום בסביבת הייצור יש לבחון את היישום בסביבת הבדיקות על מנת לבחון תקלות. יש לוודא תיעוד שינויים שמבוצעים בישום בכל שלבי הבדיקות ותהליכי בקרת כשירות (ATP).

2.2. יש לבצע בדיקת שפיות, בדיקת חדירות ובדיקת חולשות ייעודיות ליישום בענן בהתאם למורכבות המערכת ומאפייניה.

2.3. לאחר שתוקנו הליקויים (באם היו) ובהתאם לאישורו של מנהל אבטחת המידע, ניתן להעלאות את היישום לסביבת הייצור.

2.4. בהתאם לצורך, יש לבצע הדרכה לכלל העובדים בארגון הרפואי המשתמשים בשירות/ביישום הממוקם בשירותי מחשוב הענן ולכלול היבטים לשימוש מאובטח.

3. <u>ניטור אירועי אבטחת מידע ותקלות</u>

3.1. על הארגון לוודא שביכולתו לבצע ניטור אירועי אבטחת מידע הקשורים ליישום מחשוב ענן ולשימושו במערכות מחשוב ענן לאורך כל תקופת השימוש בשירותי מחשוב ענן.

3.2. על הארגון להגדיר יעדי ניטור, לרבות סוגי המידע והפעילויות שיש לנטר, סוג הניטור הנדרש, אופן שמירת נתוני הניטור, הגדרת מורשי הגישה לנתונים אלו ואופן מתן הגישה אליהם.

3.3. ניתן לבצע ניטור באמצעות כלים המסופקים ע"י ספק מחשוב הענן, אולם יש לוודא שהכלים עומדים בסטנדרטים מקובלים ומאפשרים שילוב עם מערכות הניטור הקיימות של הארגון.

4. <u>אחריות ובקרה</u>

4.1. מנהל אבטחת מידע, יחד עם מנהל מערכות המידע ואחראי תפעול תשתיות יהיו אחראיים לבצע בקרה על הפתרון המוצע, בחינת תקינותו ומעקב אחר תקלות.

4.2. מנהל אבטחת המידע יהיה אחראי לבצע סקרי סייבר ומבדקי חדירות בתחילת השימוש בשירות מחשוב ענן חדש בהתאם לתדירות הקבועה בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.

5. <u>מעקב ודיווח</u>

5.1. באחריות מנהל אבטחת המידע ומנהל מערכות המידע לנהל מעקב שוטף אחר יישום הפתרון בארגון.

5.2. מנהל אבטחת המידע ומנהל מערכות המידע ידווחו לוועדת הענן הארגונית בדבר תכנון מול ביצוע של הפתרון הנבחר ומעקב שיפור ליקויים באם נדרשו.

<u>כללי</u>

1. דיווחים על פי חוזר זה יש להעביר לכתובת המייל infosec@moh.gov.il.