1. כללי

1.1. פעילותו התקינה של המרכז לבריאות הנפש 'שער מנשה' (להלן: "ביה"ח") מושפעת ותלויה ברמת הסודיות, השלמות, הזמינות, הכלילות (Integrity) או השרידות של המידע והנכסים שבאחריות הביה"ח.

1.2. המידע, המערכות המנהלות אותו, האמצעים והציוד עליו הוא מושתת, מהווים נכס מרכזי וחיוני של הביה"ח ויש להגן עליהם כעל משאבים אחרים בעלי ערך.

1.3. פגיעה במידע תוביל לנזקים העלולים לתת אותותיהם בהיבטים תפעוליים, טכנולוגיים וכספיים וכן להוביל לפגיעה בצנעת הפרט של עובדי ולקוחות הביה"ח, ולפגיעה במוניטין ובתדמית הביה"ח.

1.4. מדיניות אבטחת המידע מבוססת על סיכוני האבטחה הדינמיים תוך התאמה לצרכים התפעוליים והארגוניים של הביה"ח. העקרונות המונחים במדיניות אבטחת המידע מהווים בסיס לנהלי העבודה בתחומי אבטחת המידע השונים.

1.5. מדיניות אבטחת המידע של ביה"ח נגזרת מתקן ניהול אבטחת המידע הבינלאומי ISO 27001:2016.

1.6. המדיניות חלה על כלל עובדי הביה"ח, ובכלל זה הן עובדים פנימיים (קבועים וזמניים) והן עובדי outsourcing, בתוך הביה"ח וכן בכל היחידות הארגוניות הכלולות במבנה הארגוני של הביה"ח.

1.7. מסמך המדיניות יפורסם ויהיה נגיש לכלל עובדי הביה"ח ובעלי עניין פנימיים וחיצוניים.

1.8. עקרונות המדיניות יועברו לעובדים במסגרת הדרכות אבטחת המידע בביה"ח.

2. מטרות מדיניות אבטחת מידע

2.1. הצגת תפיסת ההנהלה לגבי אבטחת המידע בביה"ח ושמירה על מחויבותה לנושא.

2.2. קביעת עקרונות מנחים ליישום אבטחת המידע בביה"ח, על בסיסם ניתן יהיה ליישם אמצעי אבטחה ולאורם ניתן יהיה לבחון את רמת האבטחה הקיימת.

2.3. העלאת רמת המודעות של מנהלי ועובדי הביה"ח לנושא אבטחת מידע.

2.4. הגדרת סמכויות בעלי התפקידים השונים בתחום אבטחת מידע בביה"ח.

2.5. מתן מסגרת לכלים ולתהליכים המרכזיים בביה"ח בנושאי אבטחת מידע, תוך יצירת תשתית לנהלים מקיפים בתחומים השונים.

2.6. קיום שיפור מתמיד.

3. אחריות על גיבוש והטמעת מדיניות אבטחת המידע בארגון

ועדת ההיגוי לנושא אבטחת מידע אחראית לגיבוש עקרונות המדיניות, להתוויית אסטרטגיות לפעילות, להקצאת משאבים הנדרשים ליישום המדיניות **ומימוש מטרות אבטחת מידע שהוגדרו**, לפיקוח אחר תכניות העבודה השנתיות, לקיום הערכת נזקים בעקבות תקלות ולגיבוש המלצות לטיפול ולשיפור מתמיד.

4. <u>אזכורים/סימוכין:</u>

4.1. סטנדרט JCI בתחום ניהול מידע (MOI 1, MOI 2, MOI 8.1)

4.2. תקן ISO 27001

4.3. תקן ISO 27799

5. <u>הגדרות</u>

5.1. <u>מדיניות אבטחת המידע</u> – עקרונות המפורטים במסמך מטעם הנהלת הביה"ח בו מצהירה ההנהלה לגבי מחויבויותיה בעניין עמידה בכל חוק, תקן ונוהל בהיבט אבטחת מידע.

5.2. <u>מידע</u> - כל נתון הנוגע ו/או הקשור לפעילותו, תפעולו או תפקודו של הביה"ח, לרבות מידע הנוגע לצנעת הפרט, הקיים על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרונים, על-גבי מצעי מידע פיזיים וכן מידע המועבר בעל-פה.

5.3. <u>אבטחת מידע</u> - מכלול הפעולות והאמצעים הננקטים והמיושמים בביה"ח, שמטרתם להביא לכך שהמידע ופריטי הציוד היוצרים אותו והמטפלים בו, יוגנו מפני פגיעה, חשיפה, מחיקה או שינוי, במזיד או בשוגג, הן מתוך הביה"ח והן מחוצה לו.

5.4. <u>ועדת ההיגוי לנושא אבטחת מידע</u> - פורום ניהולי שמונה ע"י מנכ"ל הביה"ח ובראשו יושבים מנכ"ל הביה"ח או מי מטעמו ונועד לאשרר ולתקף את מדיניות הביה"ח בתחום אבטחת המידע, להתוות אסטרטגיות לפעילות, לפקח אחר תכניות העבודה השנתיות, לקיים הערכת נזקים בעקבות תקלות ולגבש המלצות לטיפול.

5.5. <u>בעל מידע</u> - מנהל נכס מידע האחראי על המידע, על שינויו ו\או ההשפעה אשר תהיה לאובדנו על הפעילות הארגונית של המחלקה.

6. **<u>חלות /אחריות ביצוע:</u>**

מנהל אבטחת מידע, עובדי המרכז הרפואי ,כל אחד עפ"י תחום עיסוקו ואחריותו.

7. <u>שיטה</u>

7.1. <u>רקע:</u>

7.1.1. מערכת אבטחת המידע בארגון נדרשת לזיהוי של תהליכים ומערכות החיוניים לטיפול רפואי ואשר כשל שלהן עלול להוביל להשפעות שליליות על החולים – תהליכים ומערכות אלו יזכו לעדיפות בטיפול וההתייחסות על מנת למנוע כשל ופגיעה בפעילותן.

7.1.2. עם זאת, לצד הצורך בשמירה על המידע ואבטחתו הנהלת הארגון נדרשת לבחון והתחשב בהשלכות של אמצעי אבטחה על בטיחות החולה ואת ההשלכות של אמצעי אבטחת מידע על ביצוע מערכות מידע בריאותיות המופעלות בארגון ולנהל את הסיכונים הנוגעים בצורך לאזן בין הסכנה למידע לצורך התפעולי, בריאות ובטיחות המטופל והצוות.

<u>מנהיגות ומחויבות הנהלה לנושא אבטחת מידע</u> :

7.1.3. הנהלת המרכז לבריאות הנפש רואה את ההגנה על המידע בהיבט של שלימות, זמינות ואמינות כנושא בעל חשיבות עליונה.

7.1.4. הנהלת המרכז לבריאות הנפש תוודא שילוב משמעויות אבטחת מידע ובדגש על מידע רפואי אישי בכלל הפרויקטים הממומשים בארגון וכן תשקול את בטיחות החולה כמרכיב קריטי בעת הערכת סיכונים לפרויקט (בכל פרויקט בו מעורבים עיבוד של מידע רפואי אישי).סיכונים אלה ינותחו בקפידה תוך התייחסות באופן מפורש לזיהויים והקטנתם בשלבי תכנון הפרויקט וביצועו.

7.1.5. הנהלת המרכז לבריאות הנפש לוקחת על עצמה להוביל ולהנחיל את כלל הפעילות הנדרשת על מנת לממש הגנה ראויה על המידע כפי שמתחייב עפ"י דרישות החוק, הלקוחות, בעלי עניין, תקן iso 27001 ורגולציות מחייבות.

7.1.6. הנהלת המרכז לבריאות הנפש מתחייבת לגבות את מדיניות אבטחת המידע של הביה"ח, מתוך הכרה בחשיבות פעילויות האבטחה וראייה ניהולית הכוללת את העשייה בתחום זה.

7.1.7. הנהלת המרכז לבריאות הנפש תוודא קיומם של משאבים הולמים, ליישום, תפעול, בקרה ושיפור עקרונות האבטחה, כמוגדר ועל-פי הצורך המשתנה.

7.1.8. הנהלת המרכז לבריאות הנפש תקצה את המשאבים הנדרשים, על מנת להגן על המידע והנכסים של הביה"ח ולעמוד בדרישות מערכת ניהול אבטחת המידע (מנא"מ) בהתאם לתקן iso 27001.

7.1.9. על מנת לעמוד ביעדים שהציבה לעצמה ההנהלה בנושא אבטחת מידע, תפעל ההנהלה בדרכים הבאות:

7.1.9.1. העמדת תקציב ראוי לנושא אבטחת המידע הכולל -

7.1.9.1.1. הקמה, יישום, הפעלה, ניטור, סקירה תחזוקה ושיפור המנא"מ.

7.1.9.1.2. ווידוא כי נהלי אבטחת המידע תומכים בדרישות הרלוונטיות.

7.1.9.1.3. הגדרת דרישות המחויבות על פי דין והתחייבויות אבטחה חוזיות.

7.1.9.1.4. תחזוקת אבטחה נאותה באמצעות יישום נכון של כל אמצעי הבקרה.

7.1.9.1.5. עריכת סקרי סיכונים ומבדקים פנימיים לפי הצורך ולתגובה מתאימה לתוצאות סקרים ומבדקים אלה.

7.1.9.1.6. שיפור האפקטיביות של המנא"מ לפי הצורך.

7.1.10. שיפור מתמיד – הנהלת המרכז לבריאות הנפש מתחייבת לנקוט בכל האמצעים ע"מ לוודא שיפור מתמיד של מצב אבטחת המידע והמנא"מ.

7.1.11. בקרת תהליכים – הנהלת המרכז לבריאות הנפש מתחייבת לבצע הטמעה של דרישות מערכת ניהול אבטחת מידע במסגרת כלל תהליכי המרכז לבריאות הנפש.

7.1.12. מחויבות כלל מנהלים ועובדי המרכז לבריאות הנפש – על עובדי המרכז לבריאות הנפש להיות מודעים לסיכונים של חשיפת מידע, לנקוט את כל האמצעים כדי למנוע חשיפה ואם יתקלו באירוע חריג עליהם לדווח על כך ל*מוביל אבטחת מידע*.

7.2. <u>אחריות על אבטחת המידע בביה"ח</u> - הנהלת המרכז לבריאות הנפש הגדירה את המסגרות הארגוניות, אשר יישמו את מדיניות אבטחת המידע בביה"ח ויבקרו את אופן יישומה ובתוכם:

7.2.1. ועדת ההיגוי לנושא אבטחת מידע – מגדירה את המדיניות ואת נהלי המרכז לבריאות הנפש בתחומים הנוגעים לאבטחת מידע.

7.2.2. מוביל אבטחת מידע - אחראי על הניהול השוטף של ענייני אבטחת המידע בביה"ח.

7.2.3. נאמני אבטחת מידע במחלקות – ההנהלה מינתה נציגות אבטחת מידע ביחידות המרכז לבריאות הנפש השונות, על מנת להבטיח הטמעה מיטבית של מדיניות אבטחת המידע בכלל חלקי המרכז לבריאות הנפש.

7.2.4. שאר הגורמים האחראים על יישום, גיבוש והטמעה של מערכת ומדיניות אבטחת המידע בביה"ח

7.3. <u>הגדרת מטרות אבטחת המידע ותכנית העבודה לאבטחת מידע בביה"ח</u>:

7.3.1. מטרות אבטחת מידע של המרכז לבריאות הנפש הוגדרו ע"י ועדת ההיגוי לאבטחת המידע תוך התאמתם למדיניות אבטחת המידע, דרישות בעלי העניין ונושאי אבטחת המידע הרלוונטיים לארגון.

7.3.2. מטרות אבטחת המידע אושרו ע"י יו"ר ועדת ההיגוי או מנהל ביה"ח. שינוי/עדכון המטרות יבוצע אחת לשנה במסגרת סקר ההנהלה או בעקבות אירוע משמעותי, תוך הגדרת יעדים ומדדים בהתאם.

7.3.3. ועדת ההיגוי הגדירה לכל מטרות אבטחת המידע מדדים ויעדים לבחינת מימושן וכן הוגדרו המשימות והפעולות הנדרשות לצורך עמידה ביעדים אלו. ע"ב המשימות והפעולות הנדרשות נבנתה תכנית העבודה של המרכז לבריאות הנפש לנושא אבטחת המידע.

7.3.4. תכנית העבודה תובא לאישור ועדת ההיגוי בסקר ההנהלה השנתי בביה"ח,

7.3.5. במסגרת ועדות ההיגוי השוטפות וסיקרי ההנהלה תתבצע בקרה שוטפת בנוגע לסטטוס מימוש והעמידה בתוכנית העבודה שהוגדרה.

7.3.6.למשימות שלא בוצעו, ביצוען התעכב או משימות שלא תוכננו מראש בתוכנית העבודה - יתבצע ניתוח סיבות ומשמעויות, תוך קביעה של יו"ר ועדת ההיגוי בנוגע ללוחות זמנים, אחראים ומשאבים מעודכנים נדרשים.

7.4. <u>מטרות אבטחת מידע בביה"ח:</u>

7.4.1.הבטחת **סודיות** המידע של **מטופלי** ביה"ח ונאגר במערכות המידע, במיתקנים ובתהליכי העבודה של ביה"ח.

7.4.2.הבטחת **זמינות** המידע מערכות המידע והתשתיות לצורך המשכיות הפעילות העיסקית ומתן השירות למטופלים.

7.4.3.הבטחת **אמינות** המידע בפעילות השוטפת ובמערכות המידע, לאורך כל תהליכי העבודה ווידוא מתן תוצאות אמינות ומדויקות לכלל המטופלים.

7.4.4.הבטחת **סודיות** המידע האישי של **עובדי** ביה"ח.

7.4.5.**עמידה ברגולציות** ונושאי אבטחת מידע מחייבים.

7.4.6.העלאת **מודעות לאבטחת מידע** בקרב מנהלים ועובדים והעלאת הכשירות המיקצועית של העוסקים בתחום אבטחת המידע בביה"ח.

7.4.7.שיפור **החוסן** של מערכות המידע ורשתות המרכז בפני פגיעה בהיבט **סודיות, אמינות וזמינות** כתוצאה מפעילות זדונית ע"י גורם חיצוני או פנימי.

7.5. <u>קריטריונים לביצוע ניהול סיכונים</u>:

7.5.1. עקרונות מדיניות אבטחת המידע יתבססו על מערכת ניהול סיכונים, המזהה, מבקרת ממזערת או מונעת את סיכוני האבטחה העלולים להשפיע על המידע, מאגריו או מערכותיו.

7.5.2.ניהול הסיכונים יהיה מושתת על הערכת סיכונים המשקפת את מידת פגיעותם של המידע, מאגריו ומערכותיו, הערכת האיומים, השלכותיהם ומידת היתכנות התממשותם.

7.5.3.במערכת מנא"מ יוגדרו תהליכים וכלים הנדרשים לאבטחתם של נכסי המרכז הרפואי לבריאות הנפש, בהתאם להערכת הסיכונים.

7.6. <u>אבטחה פיזית</u> - ייושמו הגנות ובקרות פיזיות ומדיניות "שולחן נקי", על מנת למנוע פעולות אשר תוצאותיה עשויות להיות חשיפה, גניבה, שינוי או הרס של מידע. אמצעי הגנה אלו יתאימו לרמת הסיווג של המידע.

7.7. <u>אבטחת משאבי אנוש</u> - נקבעו עקרונות אבטחת מידע בכל הקשור לעובדי המרכז הרפואי לבריאות הנפש, על מנת לצמצם את הסיכונים הנובעים מבעיות במהימנות עובדים, חוסר מודעות של עובדים או רצון מכוון של עובד לפגוע במידע האגור במערכות המרכז הרפואי לבריאות הנפש.

7.8. <u>פיתוח מאובטח</u> - היבטי אבטחת מידע ישולבו בתהליכי פיתוח מערכות מידע בביה"ח, וזאת ע"מ להבטיח שדרישות אבטחת מידע מהוות חלק בלתי נפרד מכל שלבי מחזור חיים של פרויקטי פיתוח בביה"ח.

7.9. <u>רכש וספקים</u> - ייושמו היבטי אבטחת מידע בהתקשרות ועבודה עם ספקים ונותני שירות חיצוניים, וזאת ע"מ להבטיח יישום כללי אבטחת מידע בנכסי המרכז הרפואי לבריאות הנפש הניתנים לגישה של ספקים ונותני שירות חיצוניים בדגש אל מול תהליכים ושינויים בהם מעורב מידע רפואי אישי אצל גורמים צד ג'.

7.10. גיבויים - הוגדרה מדיניות לביצוע גיבויים שמטרתה להבטיח שסוגי המידע השונים הקיימים בביה"ח מזוהים, וכי קיימות דרישות גיבוי לכל סוג של מידע התאם לרגישותו על מנת להבטיח את אמינותו, שלמותו, זמינותו וכלילותו (Integrity).

7.11. בקרת גישה - ע"מ למנוע גישת גורמים לא מורשים למערכות ומאגרי המידע, הוגדרו כללים ועקרונות למתן ובקרת גישה למערכות המידע ולרשת המרכז הרפואי.

7.12. שילוב מנגנוני הצפנה - נקבעו עקרונות לשילוב מנגנוני הצפנה במערכות המרכז לבריאות הנפש, על מנת להגן על סודיות ושלמות מאגרי מידע רגישים מפני חשיפה ושינוי ע"י גורמים לא מורשים.

7.13. עבודה מרחוק - הוגדרו כללים והנחיות אבטחת מידע בנוגע לגישת עובדי הביה"ח וגורמים חיצוניים לרשת הביה"ח מרחוק ובמסגרת שימוש באמצעי מחשוב ניידים.

7.14. אבטחת אמצעי מחשוב ניידים :

7.14.1. הוגדרו העקרונות, השיטה, תהליכי העבודה והאמצעים ע"מ לאפשר שימוש מאובטח במחשבים נישאים/ניידים בביה"ח ולמנוע פגיעה בשלמות, אמינות, זמינות, סודיות ושרידות המידע המאוחסן עליהם.

7.14.2. אבטחת המידע בביה"ח תיושם בכפוף ובצמידות לחוקי מדינת ישראל הנוגעים לתחום אבטחת המידע, לרבות חוק המחשבים, חוק הגנת הפרטיות ותקנותיו, תקן ניהול אבטחת המידע, ISO 27001 ובהתייחס להחלטות ועדת היגוי לנושא אבטחת מידע.

7.15. בקרה -

7.15.1. ועדת ההיגוי לנושא אבטחת מידע תבצע סקירה של ישימות מדיניות אבטחת המידע במסגרת סקר הנהלה, כולל בחינת העמידה בתוכנית העבודה, סקירת הסיכונים הקיימים וקבלת אישור ההנהלה לסיכונים / הסיכונים השיוריים, סקירת אירועי אבטחת המידע שהיו בביה"ח, סקירת תוצאות המבדקים הפנימיים, סקירת תוצאות סקרי הסיכונים של המערכות, בדיקת סטאטוס הטיפול בנושאים עליהם הוחלט במפגש הקודם, דיון בכל נושא אשר יועלה ע"י המשתתפים.

7.15.2. תבוצע סקירה תקופתית שנתית או סקירה לאחר שינוי משמעותי ע"י גורם בלתי תלוי של מסמכי מדיניות אבטחת מידע. סקר המדיניות יבחן את התאמת המדיניות מול השגת המטרות ובמיוחד מול שינויים בתהליכים הארגוניים, במערכות המידע והתשתיות ושינויים במעורבות גופי צד ג התהליכים וכן בעקבות אירוע משמעותי.

הנהלת ביה"ח רואה בכלל המנהלים והעובדים שותפים מלאים למאמץ להגנה על המידע ומצפה לשיתוף פעולה ביישום המדיניות והכללים הנגזרים ממנה.