תקציר מדיניות אבטחת מידע **המרכז הרפואי "זיו"**	

אל: <u>רשימת תפוצה.</u>

הנדון: **<u>תקציר מדיניות אבטחת המידע במרכז הרפואי זיו</u>**

1. רקע

1.1. **פעילותו התקינה של ביה"ח זיו (להלן: "ביה"ח") מושפעת ותלויה ברמת הסודיות, השלמות, הזמינות, הכלילות (Integrity) או השרידות של המידע והנכסים שבאחריות ביה"ח.**

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

1.3. **פגיעה במידע תוביל לנזקים העלולים לתת אותותיהם בהיבטים תפעוליים, טכנולוגיים וכספיים וכן להוביל לפגיעה בצנעת הפרט של אזרחי המדינה, לפגיעה במוניטין ובתדמית ביה"ח והמדינה.**

1.4. **מדיניות אבטחת המידע מבוססת על סיכוני האבטחה הדינמיים תוך התאמה לצרכים התפעוליים והארגוניים של ביה"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 ISO27799 ותקן ISO 27001:2013.**

2. מנהיגות ומחויבות הנהלה לנושא אבטחת מידע **- הנהלת בית החולים (להלן: "ההנהלה") רואה את ההגנה על המידע בהיבט של שלימות, זמינות ואמינות כנושא בעל חשיבות עליונה. . הנהלת ביה"ח לוקחת על עצמה להוביל ולהנחיל את כלל הנושאים והפעילויות הנדרשות על מנת לממש הגנה ראויה על המידע כפי שמתחייב עפ"י דרישות החוק, תקן iso 27001 ו- iso27799 ונהלי מב"ר.**

3. **הנהלת ביה"ח תקצה את המשאבים הנדרשים, על מנת להגן על המידע ועל הנכסים של בית החולים ולעמוד בדרישות מערכת ניהול אבטחת המידע (מנא"מ) כפי שמתחייב בתקנים ISO 27799 ו- 27001 ISO.**

על עובדי בית החולים זיו להיות מודעים לסיכונים של חשיפת מידע, לעשות את כל האמצעים כדי למנוע חשיפה ואם יתקלו באירוע חריג עליהם לדווח על כך לגורמי אבטחת המידע בביה"ח.

4. להלן מטרות אבטחת מידע בבית החולים:

4.1. **הבטחת סודיות המידע הרפואי החסוי והחסוי ביותר של לקוחות ביה"ח המטופל ונאגר במערכות המידע ומתקני בית החולים.**

4.2. **הבטחת זמינות המידע מערכות המידע לצורך המשכיות הפעילות העסקית ומתן השירות ללקוחות.**

4.3. **הבטחת אמינות המידע לאורך כל תהליכי העבודה בביה"ח ווידוא מתן תוצאות אמינות ומדויקות לכלל הלקוחות.**

4.4. **אבטחת וחיסיון המידע האישי של עובדי ביה"ח.**

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

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

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

5. עיקרי שיטת הערכת הסיכונים **- עקרונות מדיניות אבטחת המידע יתבססו על מערכת ניהול סיכונים, המזהה, מבקרת ממזערת או מונעת את סיכוני האבטחה העלולים להשפיע על המידע, מאגריו או מערכותיו.**

6. אחריות על אבטחת מידע בבית החולים – **הנהלת בית החולים הגדירה את הגורמים והמסגרות הארגוניות, אשר באחריותם ליישם את מדיניות אבטחת המידע בביה"ח:**

- **ועדת היגוי לנושא אבטחת מידע** – מגדירה את מדיניות ונהלי ביה"ח בתחומים הנוגעים לאבטחת מידע.
- **ממונה על אבטחת מידע** - הממונה על אבטחת המידע בבית החולים אחראי על הניהול השוטף של ענייני אבטחת מידע בבית החולים.
- **נאמני אבטחת מידע במחלקות** – ההנהלה מינתה נציגות אבטחת מידע ביחידות ביה"ח השונות, על מנת להבטיח הטמעה מיטבית של מדיניות אבטחת המידע בכלל חלקי בית החולים.
- **עובדי בית החולים** - על כלל עובדי ביה"ח חלה אחריות אישית בכל הנוגע לשמירה על אבטחת המידע וחסיונו.

7. על מנת לממש את אחריותה ומחויבותה של ההנהלה לנושא אבטחת המידע הוגדרו ונקבעו הכללים לטיפול בנושאים הבאים :

א. **אבטחה לוגית** - האבטחה הלוגית מהווה את ה"שכבה" העיקרית והקרובה ביותר בהגנה על המידע המצוי במערכות המחשב והתקשורת. ממונה אבטחת המידע בבית החולים יתווה את רמת האבטחה הלוגית המחייבת עבור רכיביהן השונים של מערכות המחשוב והתקשורת. תיושם מדיניות הרשאות ובקרת גישה למידע רפואי בהתאם לתפקיד והצורך המקצועי.

ב. **אבטחה פיזית** - ייושמו הגנות ובקרות פיזיות, על מנת למנוע פעולות אשר תוצאותיה עשויות

להיות חשיפה, גניבה, שינוי או הרס של מידע. אמצעי הגנה אלו יתאימו לרמת הסיווג של המידע.

ג. **אבטחת משאבי אנוש** – נקבעו עקרונות אבטחת מידע בכל הקשור לעובדי בית החולים, על מנת לצמצם את הסיכונים הנובעים מבעיות במהימנות עובדים, חוסר מודעות של עובדים או רצון מכוון של עובד לפגוע במידע האגור במערכות בית החולים.

ד. **פיתוח מאובטח** – הוגדרו היבטי אבטחת מידע ששולבו בתהליכי פיתוח מערכות מידע.

ה. **רכש וספקים** –מיושמים היבטי אבטחת מידע בתקשורת ועבודה עם ספקים חיצוניים .

ו. **גיבויים** – במרכז הוגדרו תהליכים להבטחת אמינות, שלמות, זמינות וכלילות (Integrity) המידע, וזאת ע״מ להבטיח שסוגי המידע השונים הקיימים בבית החולים מזוהים, וכי דרישות גיבוי לכל סוג של מידע מוגדרות בהתאם לרגישות המידע .

ז. **בקרת גישה** – נקבעו כללים ועקרונות למתן גישה ולמערכות המידע ובקרה אחר התחברות לרשת .

ח. **שילוב מנגנוני הצפנה** – בבית החולים פותחו עקרונות לשילוב מנגנוני הצפנה במערכות החברה, על מנת להגן על מידע רגיש מפני חשיפה ושינוי.

ט. **עבודה מרחוק** – בבית החולים נקבעו כללים והנחיות אבטחת מידע לגישת עובדי ביה״ח וגורמים חיצוניים לרשת החברה מרחוק.

י. **אבטחת אמצעי מחשוב ניידים** – מבוצע יישום העקרונות, השיטה, תהליכי העבודה והאמצעים ע״מ לאפשר שימוש מאובטח במחשבים נישאים /ניידים ולמנוע פגיעה בשלמות, אמינות, זמינות, סודיות ושרידות המידע המאוחסן על גבי מחשבים ניידים בארגון.

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