תמצית מדיניות אבטחת המידע של המרכז הרפואי בני ציון

1. רקע

1.1. פעילותו התקינה של המרכז הרפואי בני ציון (להלן: "המרכז הרפואי") מושפעת ותלויה ברמת הסודיות, השלמות, הזמינות, הכלילות (Integrity) או השרידות של המידע והנכסים שבאחריות המרכז הרפואי.

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

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

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

1.5. מדיניות אבטחת המידע של המרכז הרפואי נגזרת מתקן ניהול אבטחת המידע הבינלאומי ISO 27799:2016 ותקן ISO 27001:2013.

2. מנהיגות ומחויבות הנהלה לנושא אבטחת המידע

2.1. הנהלת המרכז הרפואי בני ציון (להלן: "ההנהלה") רואה את ההגנה על המידע בהיבט של שלימות, זמינות ואמינות כנושא בעל חשיבות עליונה.

2.2. הנהלת המרכז הרפואי לוקחת על עצמה להוביל ולהנחיל את כלל הנושאים והפעילויות הנדרשות על מנת לממש הגנה ראויה על המידע כפי שמתחייב עפ"י דרישות החוק ותקן ISO 27799 ו- ISO 27001.

2.3. הנהלת המרכז הרפואי תקצה את המשאבים הנדרשים, על מנת להגן על המידע ועל הנכסים של המרכז הרפואי ולעמוד בדרישות מערכת ניהול אבטחת המידע (מנא"מ) כפי שמתחייב בתקן ISO 27799 ו- ISO 27001.

2.4. על עובדי המרכז הרפואי להיות מודעים לסיכונים של חשיפת מידע, לעשות את כל האמצעים כדי למנוע חשיפה ואם יתקלו באירוע חריג עליהם לדווח על כך לגורמי אבטחת המידע במרכז הרפואי.

3. להלן מטרות אבטחת מידע במרכז הרפואי

3.1. הבטחת סודיות המידע הרפואי האישי של מטופלי המרכז הרפואי, המצוי במחלקות ובתהליכי העבודה, ונאגר במערכות המידע ובמתקני המרכז הרפואי.

3.2. הבטחת זמינות המידע ומערכות המידע לצורך המשכיות הפעילות העסקית ומתן השירות למטופלים ולמחלקות המרכז הרפואי.

3.3. הבטחת אמינות המידע לאורך כל תהליכי העבודה במרכז הרפואי ווידוא מתן תוצאות אמינות ומדויקות לכלל הלקוחות/מטופלים.

3.4. אבטחת המידע העסקי הרלוונטי לפעילות המרכז רפואי.

3.5. אבטחת וחיסיון המידע האישי של עובדי המרכז רפואי.

3.6. עמידה ברגולציות ונושאי אבטחת מידע מחייבים.

3.7. העלאת המודעות לאבטחת מידע בקרב מנהלים ועובדים, והעלאת הכשירות המקצועית של העוסקים בתחום אבטחת המידע במרכז הרפואי.

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

4. <u>עיקרי שיטת הערכת הסיכונים</u>

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

5. <u>אחריות על אבטחת המידע במרכז הרפואי</u>

5.1. הנהלת המרכז הרפואי הגדירה את הגורמים והמסגרות הארגוניות, אשר באחריותם ליישם את מדיניות אבטחת המידע במרכז רפואי:

5.1.1. ועדת היגוי לנושא אבטחת מידע – מגדירה את מדיניות ונהלי המרכז הרפואי בתחומים הנוגעים לאבטחת מידע.

5.1.2. ממונה אבטחת מידע - ממונה אבטחת מידע במרכז הרפואי אחראי על הניהול השוטף של ענייני אבטחת המידע במרכז הרפואי.

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

5.1.4. מנהלי ועובדי המרכז הרפואי - על כלל מנהלי ועובדי המרכז הרפואי חלה אחריות אישית בכל הנוגע לשמירה על אבטחת המידע וחסיונו.

6. <u>על מנת לממש את אחריותה ומחויבותה של ההנהלה לנושא אבטחת המידע הוגדרו ונקבעו כללים לטיפול בנושאים הבאים:</u>

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

6.2. אבטחה פיזית - ייושמו הגנות ובקרות פיזיות, על מנת למנוע פעולות אשר תוצאותיהן עשויות להיות חשיפה, גניבה, שינוי או הרס של מידע. אמצעי הגנה אלו יתאימו לרמת הסיווג של המידע.

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

6.4. פיתוח מאובטח – הוגדרו היבטי אבטחת מידע ששולבו בתהליכי פיתוח מערכות מידע.

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

6.6. גיבויים – במרכז הרפואי הוגדרו תהליכים להבטחת אמינות, שלמות, זמינות וכלילות (Integrity) המידע, וזאת ע"מ להבטיח שסוגי המידע השונים הקיימים במרכז הרפואי מזוהים, וכי דרישות הגיבוי לכל סוג של מידע מוגדרות בהתאם לרגישות המידע.

6.7. בקרת גישה – נקבעו כללים ועקרונות למתן גישה למערכות המידע ובקרה אחר התחברות לרשת.

6.8. שילוב מנגנוני הצפנה – במרכז הרפואי פותחו עקרונות לשילוב מנגנוני הצפנה במערכות המרכז הרפואי, על מנת להגן על מידע רגיש מפני חשיפה ושינוי.

6.9. עבודה מרחוק – במרכז הרפואי נקבעו כללים והנחיות אבטחת מידע לגישת עובדי המרכז הרפואי וגורמים חיצוניים לרשת המרכז הרפואי מרחוק.

6.10. 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 במרכז הרפואי.

7. הנהלת המרכז הרפואי רואה בכלל המנהלים והעובדים שותפים מלאים למאמץ להגנה על המידע ומצפה לשיתוף פעולה ביישום המדיניות והכללים הנגזרים ממנה.