

מהדורה 1	 המרכז לבריאות האישה Health Center for Women Ramat Aviv   רמת אביב
בתוקף דצמבר 2016	<b>מדיניות אבטחת המידע</b>
עמוד 1 מתוך 2	

## תקציר מדיניות אבטחת המידע במרכז לבריאות האישה

1. **מחויבות הנהלה לנושא אבטחת מידע** - הנהלת המרכז לבריאות האישה (להלן: "ההנהלה") רואה את ההגנה על המידע בהיבט של שלימות, זמינות ואמינות כנושא בעל חשיבות עליונה. הנהלת המרכז תקצה את המשאבים הנדרשים, על מנת להגן על המידע בכדי לעמוד בדרישות מערכת ניהול אבטחת המידע (מנא"מ) כפי שמתחייב בתקן ISO27799 ו ISO27001 ובדרישות חוק רלוונטיות בתחום הרשומות הרפואיות, ההגנה על הפרטיות ומאגרי המידע.
 

על עובדי מנג'נט להיות מודעים לסיכונים של חשיפת מידע, לעשות את כל האמצעים כדי למנוע חשיפה ואם יתקלו באירוע חריג עליהם לדווח על כך לגורמים הממונים על אבטחת המידע במרכז לבריאות האישה.
2. **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.
3. **אחריות על אבטחת מידע במרכז לבריאות האישה** – הנהלת מנג'נט הגדירה את הגורמים והמסגרות הארגוניות, אשר באחריות ליישם את מדיניות אבטחת המידע במרכז לבריאות האישה.
  - **ועדת היגוי לנושא אבטחת מידע** – מגדירה את המדיניות והנהלים בתחומים הנוגעים לאבטחת מידע.
  - **ממונה על אבטחת מידע** - הממונה על אבטחת המידע במרכז לבריאות האישה אחראי על הניהול השוטף של ענייני אבטחת מידע.
  - **עובדי מנג'נט** – עובדי מנג'נט – על כלל עובדי החברה חלה אחריות אישית בכל הנוגע לשמירה על אבטחת המידע וחסיונו.
4. **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 במרכז לבריאות האישה יתווה את רמת האבטחה הלוגית המחייבת עבור רכיביהן השונים של מערכות המחשב והתקשורת. תיושם מדיניות הרשאות ובקרת גישה למידע רפואי בהתאם לתפקיד והצורך המקצועי.
  - ב. **אבטחה פיזית** - ייושמו הגנות ובקורות פיזיות, על מנת למנוע פעולות אשר תוצאותיהן 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 לעובדים, על מנת לצמצם את הסיכונים הנובעים מבעיות במהימנות עובדים, חוסר מודעות של עובדים או רצון מכוון של עובד לפגוע במידע האגור במערכות הארגון.

מהדורה 1	 <p>המרכז לבריאות האישה Health Center for Women Ramat Aviv   רמת אביב</p>
בתוקף דצמבר 2016	<b>מדיניות אבטחת המידע</b>
עמוד 2 מתוך 2	

- ד. **רכש וספקים** – מיושמים היבטי אבטחת מידע בתקשורת ועבודה עם ספקים חיצוניים .
- ה. **גיבויים** – בארגון הוגדרו תהליכים להבטחת אמינות, שלמות, זמינות וכלילות (Integrity) המידע, וזאת ע"מ להבטיח שסוגי המידע השונים הקיימים מזוהים, וכי דרישות גיבוי לכל סוג של מידע מוגדרות בהתאם לרגישות המידע .
- ו. **בקרת גישה** – נקבעו כללים ועקרונות למתן גישה ולמערכות המידע ובקרה אחר התחברות לרשת .
- ז. **עבודה מרחוק** – במרכז לבריאות האישה נקבעו כללים והנחיות אבטחת מידע לגישת עובדים וגורמים חיצוניים לרשת החברה מרחוק.
- ח. **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 מנגינט רואה בכלל העובדים שותפים מלאים למאמץ להגנה על המידע ומצפה לשיתוף פעולה ביישום המדיניות והכללים הנגזרים ממנה. ההנהלה מחויבת לשיפור מתמיד של מערכת ניהול אבטחת המידע ותציב יעדים שאפתניים לצורך קידום תהליך שיפור זה.

נחתם ע"י

\_\_\_\_\_  
תאריך

\_\_\_\_\_  
מנכ"ל