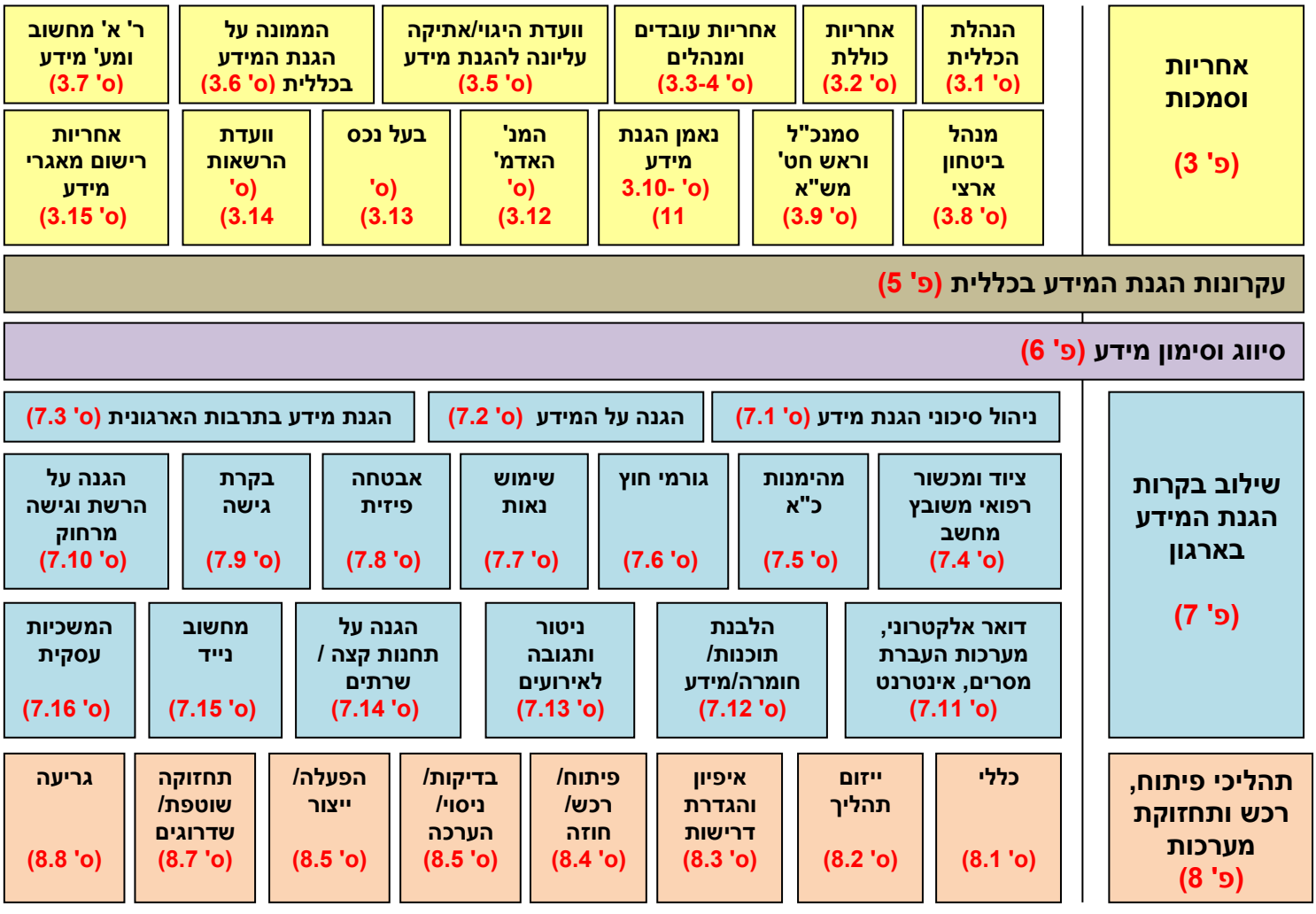
מפת נוהל מדיניות הגנת המידע בכללית				
מספר נוהל	08-01-01	תאריך אישור	28 ביולי 2015	תאריך עדכון	- - -
נושאים ותתי נושאים	• **הגנת המידע** | מדיניות הגנת המידע				
סווג בהתאם לאקרדיטציה	MOI.2 5ed, MOI.7 5ed				
גורם מפיץ	הממונה על הגנת המידע בכללית, חטיבת הלוגיסטיקה, תשתיות ומערכות מידע				
קהל היעד	כל עובדי הכללית וחברות הבת				

סוגיות מרכזיות בנוהל	
סוג המסמך	נוהל
מטרות המסמך	מטרת מסמך זה הנה להגדיר, לפרט ולהבהיר לכל מנהל/ת ועובד/ת בכללית וחברות בנות, ולכל שותף עסקי את חשיבות אבטחת והגנת המידע בארגון, את מדיניות ההנהלה בנושא זה וכן את נוהלי קיומה על מנת שהמידע על כל היבטיו יהיה אמין, זמין, חסוי ומבוקר.
הגדרות	ראה סעיף הגדרות ומונחים.
הנחיות/ טפסים.	ראה סעיף מסמכים ישימים.
שינויים מגרסה קודמת	ראה סעיף 1.1.3. אישור הנוהל לראשונה 6/6/2003, עדכון מהותי 27/10/2009, עדכון מהותי 28/7/2015.
חשוב לדעת	i. עובדי הכללית אחראים על הגנת המידע, כל אחד בתחום עבודתו. ii. עובד שגילה או שהובא לידיעתו כי נגרמה פגיעה בהגנת המידע ידווח על כך, ללא דיחוי, למנהלו הישיר ולמנהל הביטחון במוסד. iii. כל מנהל בארגון אחראי על קיום המדיניות והוראת עבודה להגנת המידע, ע"י העובדים הכפופים לו, וכך גם לגבי המידע המצוי באחריותו.

תרשים תהליך



מדיניות הגנת המידע בכללית

<u>תקציר הנוהל</u>

המידע והידע בשירותי בריאות כללית (להלן הכללית) הנם נכס המאפשר את פעילות הארגון, שמירה על רמה מקצועית, שירות לקוחות ייחודי ומוניטין.
חוקי המדינה מחייבים אותנו להגן על *"מידע רגיש" ולאבטח אותו.
מדיניות **הגנת המידע בכללית כפי שבאה לידי ביטוי בנוהל זה, מחייבת כל עובד בתחום אחריותו וכל מנהל כלפי העובדים הכפופים לו בכללית, להגן על המידע ולאבטח אותו.
פרוט הנושאים במסמך המדיניות: עקרונות יסוד, רגישות וסיווג המידע, הגדרת אחריות להגנת מידע, שילוב הגנת מידע בכללית, הגנת מידע בתהליכים, תקציב, הוצאת מידע מחוץ לארגון, הגנת מידע בתרבות הארגונית, מהימנות כ"א, שימוש לצרכים פרטיים, חיבור ב"גישה מרחוק", חובת דיווח, דואר אלקטרוני ואינטרנט.
מדיניות הגנת מידע – הנה מסמך פנימי ואין לעשות בו שימוש כלשהו מחוץ לכללית.
בשל שינוי באיומים על המידע וצורך להתייחס לאיומי Cyber, עבר מסמך זה עדכון משמעותי. השינוי חייב החלפת כל מסמך המדיניות שעודכן באוקטובר 2009 ובא במקומו.

* " מידע רגיש " – כהגדרתו בחוק הגנת הפרטיות התשמ"א 1981.
** ביולי 2009 הוחלט לשנות את השם "אבטחת מידע" ל"הגנת מידע". נוהל זה עודכן בהתאם לשינוי.

אושר ע"י: **אינגי יצחק מרום** סמנכ"ל, ראש חטיבת לוגיסטיקה, תשתיות ומערכות מידע	חתימה:
נכתב ע"י: איציק כוכב הממונה על הגנת המידע בכללית, חטיבת לוגיסטיקה, תשתיות, ומערכות מידע	

תוכן העניינים

הנושא	עמוד
1. כללי	4
2. מסמכים ישימים	5
3. אחריות וסמכות	5
4. הגדרות ומונחים	11
5. עקרונות הגנת המידע בכללית	14
6. סיווג וסימון מידע	17
7. שילוב בקרות הגנת המידע בארגון	18
8. תהליכי פיתוח, רכש ותחזוקת מערכות	28

1. כללי

1.1 מבוא

1.1.1 הגנת מידע בארגוני הבריאות במדינת ישראל נדרשת מכורח חוקי ודיני המדינה, ונוועדה להגן בעיקר על פרטיות וזכויות האדם וכן של נותני השירותים הבריאותיים, הפיננסיים, הטכנולוגיים והעסקיים במסגרת הארגון. קיימת חשיבות רבה בהגנת מידע כדי לאפשר לגלגלי העשייה לפעול ללא פגיעה בתדמית ובשירות המוגש ללקוחות.

1.1.2 ככלל, מדיניותה של הכללית היא לעמוד בכל הדרישות החוקיות, הרגולטוריות והחוזיות להגנת המידע ושמירה על הפרטיות. הכללית מתחייבת להנחיל את חובת הגנת המידע ומדיניות הגנת המידע לכל העובדים בכללית וחברות הבת.

1.1.3 מסמך זה הינו גרסה שלישית של המדיניות, מעדכן ומבטל את מסמך מדיניות הגנת המידע בכללית (נוהל 08-01-01 שעודכן לאחרונה ב- 27/9/2009) ובא במקומו.

1.2 תחולה

1.2.1 מדיניות זו חלה על כלל המידע, כהגדרתו בנוהל זה, שנוצר, מאוחסן, מעובד, מנוהל, או משונע בכללית, לרבות המערכות או המכשור המעורבים בכך.

1.3 מטרות הנוהל

1.3.1 מטרת מסמך זה הנה להגדיר, לפרט ולהבהיר לכל מנהל/ת ועובד/ת בכללית וחברות בנות, ולכל שותף עסקי את חשיבות אבטחת והגנת המידע בארגון, את מדיניות ההנהלה בנושא זה וכן את נוהלי קיומה על מנת שהמידע על כל היבטיו יהיה אמין, זמין, חסוי ומבוקר.

1.4 חלות

1.4.1 כל עובדי הכללית וחברות הבת.

1.5 מילות מפתח

* אבטחת/הגנת מידע	* סיווג מידע	* רשומה/מסמך
* הרשאה	*תהליך/פרויקט	* הצפנה

2. מסמכים ישימים

2.1. הוראות הדין (לרבות חוקים, תקנות ונהלים) אשר עניינם בהגנה על מידע והנוגעים בהגנת הפרטיות, ובכלל זה, אך מבלי לגרוע מכלליות האמור, חוק יסוד: כבוד האדם וחירותו, חוק הגנת הפרטיות, חוק זכויות החולה, חוק המחשבים, וכיוב'.

2.2. נוהל מסירת מידע רגיש בכללית מס' 08-01-02.

2.3. תקן להגנת המידע ISO 27799.

2.4. תקן אבטחת מידע למערכות בריאות, ISO 27799.

2.5. תקנPCI - אבטחת מידע בכרטיסי אשראי.

2.6. הוראות ותקנות משרד הבריאות ובפרט, חוזר מנכ"ל 3/2015 בעניין הגנה על מידע במערכות ממוחשבות במערכת הבריאות.

3. אחריות וסמכות

3.1. **אחריות ההנהלה**

3.1.1. הנהלת הכללית קובעת את מדיניות הגנת המידע בכללית ומאשרת אותה.

3.1.2. האחריות הכוללת על ניהול סיכוני הגנת המידע בכללית ובמוסדותיה חלה על ההנהלה הבכירה של הכללית / המוסד, לפי העניין.

3.1.3. אחת לשנה, הנהלת הכללית, תייחד דיון לנושא הגנת המידע בארגון. בדיון יידונו, בין היתר, הנושאים הבאים:

א. מצב הגנת המידע בכללית

ב. מיפוי והערכת הסיכונים

ג. אירועי אבטחת מידע

ד. מעבר על סקרי ת"י 27799 הפנימיים

ה. מעקב אחר יישום תוכניות לתיקון ליקויי האבטחה שהתגלו ובפרט, ליקויים שצוינו בדוחות בקורת

ו. תוכנית עבודה שנתית בתחום הגנת המידע

ז. בקרת הרשאות במערכות

ח. המשכיות עסקית, גיבויים

ט. חינוך ומודעות להגנת מידע

י. תקצוב תוכנית אבטחת המידע

3.2. **<u>אחריות כוללת</u>**

3.2.1. האחריות הכוללת לשילוב הגנת המידע בכללית וביצוע ביקורת על יישום מדיניות זו חלה על סמנכ"ל וראש חטיבת לוגיסטיקה, תשתיות ומערכות מידע.

3.3. **<u>אחריות אישית</u>**

3.3.1. עובדי הכללית אחראים על הגנת המידע, כל אחד בתחום עבודתו.

3.3.2. הנהלת הכללית קובעת רמה נאותה של מודעות, ידע וכישורים, הנחוצים לעובד בכדי לקיים הגנה אפקטיבית על המידע, בהתאם לקבוע במדיניות זו ובהוראות העבודה הרלבנטיות.

3.3.3. עובד שגילה או שהובא לידיעתו כי נגרמה פגיעה בהגנת המידע ידווח על כך, ללא דיחוי, למנהלו הישיר ולמנהל הביטחון במוסד. שני האחרונים יעבירו דיווח על התקלה לממונה על הגנת המידע בכללית ולנאמן הגנת מידע מוסדי. בכל מקרה של תקלת אבטחת מידע במערכות ממוחשבות יש לדווח <u>ללא דיחוי</u> למנהל המחשוב המוסדי. מנהל המחשוב המוסדי יעביר דיווח, <u>ללא דיחוי</u>, לאגף מחשוב ומערכות מידע ואל הממונה על הגנת המידע בכללית.

3.4. **<u>אחריות מנהלים</u>**

3.4.1. כל מנהל בארגון אחראי על קיום המדיניות והוראת עבודה להגנת המידע, ע"י העובדים הכפופים לו, וכך גם לגבי המידע המצוי באחריותו.

3.4.2. כל מנהל מוסד אחראי על עמידה בתקן ISO 27799 ביחידות הכפופות לו.

3.4.3. מנהל המחשוב, בכל מוסד וחברת בת, אחראי על יישום מדיניות זו במערכות המידע שתחת אחריותו ואלו הפועלות במוסד שלו.

3.4.4. אחריות לסימון סיווג רמת רגישות המידע – האחריות על סימון סיווג רמת רגישות המידע, חלה על כל מחבר או יוזם המידע. סיווג רמת רגישות המידע יצוין במקום בולט בכל מופע של עיון במידע.

3.5. **<u>וועדת היגוי / אתיקה עליונה להגנת מידע</u>**

3.5.1. מנכ"ל הכללית ימנה את וועדת ההיגוי / אתיקה העליונה להגנת מידע בכללית.

3.5.2. וועדת אתיקה עליונה להגנת מידע תקבע קריטריונים של טיפול אחיד ומאובטח במידע הרפואי הרגיש של שרותי בריאות כללית וחברות הבת. הוועדה תבסס החלטותיה על מדיניות נוהל זה, חוק הגנת הפרטיות התשמ"א-1981 וחוקים הנוגעים לטיפול במידע הרפואי והוראות משרד הבריאות בדבר שמירת סודיות רפואית. כל זאת בהתחשב בצורכי הארגון והדגשים בתוכנית העבודה השנתית.

3.5.3. בסמכות הוועדה לטפל בכל סוג מידע רפואי, לרבות מידע רפואי ממנו ניתן לזהות אדם פלוני ו/או "מידע רגיש" כהגדרתו בחוק הגנת הפרטיות התשמ"א-1981, פרק ב', סעיף

7. החלטות הוועדה יפורסמו באמצעות החוזר המרוכז כהנחיות/הוראות עבודה מחייבות.

3.5.4. לוועדה סמכות לשנות סיווג רמת רגישות של מידע.

3.5.5. הוועדה תורכב מ 12 חברים לפחות מכל מגזרי הארגון. יו"ר הוועדה רשאי לזמן מומחים או יועצים בהתאם לעניין. הרכב הוועדה:

א. יו"ר הוועדה – הרופא הראשי בשירותי בריאות כללית.

ב. מזכיר הוועדה - הממונה על הגנת המידע בכללית.

ג. חברי הוועדה – סמנכ"ל וראש חטיבת לוגיסטיקה, תשתיות ומערכות מידע, הממונה על הגנת המידע בכללית, ראש אגף מחשוב ומערכות מידע, מנהל ביטחון ארצי, נציג חט' בתי החולים, נציג חט' הקהילה, נציג חט' לוגיסטיקה, תשתיות ומערכות מידע, נציג חט' הכספים, נציג חטיבת שרות וקישרי לקוחות, נציג האחות הראשית, נציג הרופא הראשי, נציג חטיבת משאבי אנוש, נציג בתי החולים, נציג המחוזות, נציג מכל חברת בת, נציג היועץ המשפטי, נציג מבקר הכללית.

3.5.6. האחריות על כינוס הוועדה היא על מזכיר הוועדה. הוועדה תוכל להתכנס בנוכחות חלקית של יו"ר הוועדה או ממלא מקומו ועוד 6 חברי הוועדה. רשאי המזכיר לקבל החלטות בשם הוועדה בנושאים שיוגדרו מראש ע"י הוועדה. יכולה הוועדה לקבל החלטה בהתייעצות טלפונית / שיחת וידאו עם לפחות 6 מחברי הוועדה.

3.5.7. יו"ר וועדת האתיקה ישמש כערכאת ערעור להנחיות מקצועיות של הממונה על הגנת המידע בכללית.

3.5.8. יו"ר וועדת האתיקה יציג למנכ"ל הכללית דו"ח הערכת מצב הגנת המידע בארגון אחת לשנה.

3.5.9. החלטות הוועדה יועברו לאישור המנכ"ל.

3.6. **<u>הממונה על הגנת המידע בכללית</u>**

3.6.1. מנכ"ל הכללית ימנה ממונה על הגנת המידע ארגוני.

3.6.2. הממונה על הגנת המידע בכללית ישמש כמנחה מקצועי בתחום לכל הארגון וחברות בת.

3.6.3. הנחיות הממונה על הגנת המידע בכללית (במגבלות המדיניות) מחייבות את כלל הארגון ויש לציית להן. בנושאים הקשורים באבטחת מערכות המידע, בכללית, ממונה הגנת המידע הוא המנחה המקצועי הארגוני.

במקרים בהם ההנחיה המקצועית איננה נכונה לביצוע, על פי שיקול דעתו של ראש אגף מחשוב ומערכות מידע, יודיע על כך ראש אגף המחשוב לממונה על הגנת המידע, ועד

להסכמה בנושא (או עד לקבלת הנחיה אחרת מסמנכ"ל לוגיסטיקה תשתיות ומערכות מידע) יפעל על פי השיקולים התפעוליים הארגוניים.

3.6.4. ניתן לערער על דרישותיו של הממונה על הגנת המידע בכללית בפני יו"ר וועדת האתיקה העליונה להגנת מידע, או בפני סמנכ"ל וראש חטיבת לוגיסטיקה, תשתיות ומערכות מידע. הפניה לערעור היא באחריות הגורם המערער.

3.6.5. הממונה על הגנת המידע בכללית אחראי על פיתוח שיטות הטמעה והדרכה, התווית הוראות עבודה להגנת מידע, בקרה וביקורת על יישום הגנת המידע הכולל.

3.6.6. הממונה על הגנת המידע בכללית יקבע דרישות הגנת מידע בתהליך חדש/שינוי גרסה, יקיים קשר בנושא עם גורמים חיצוניים בתחומי הידע הרלוונטים.

3.6.7. הממונה על הגנת המידע בכללית יהיה אחראי על הפעלת "מודול הממונה על הגנת המידע בכללית" במרכז לאיתור וטיפול באירועי תקלה/פגיעה בהגנת המידע (SOC).

3.6.8. הממונה על הגנת המידע בכללית יהיה אחראי על מדיניות ובקרת המשתמשים והרשאות לכלל המערכות הארגוניות.

3.6.9. הממונה על הגנת המידע בכללית אחראי על הטמעת נושא הגנת המידע בכללית בסיוע חטיבת משאבי אנוש.

3.7. **<u>ראש אגף מחשוב ומערכות מידע</u>**

במקרים בהם ההנחיה המקצועית של הממונה על הגנת המידע איננה נכונה לביצוע, על פי שיקול דעתו של ראש אגף מחשוב ומערכות מידע, יודיע על כך ראש אגף המחשוב לממונה על הגנת המידע, ועד להסכמה בנושא (או עד לקבלת הנחיה אחרת מסמנכ"ל לוגיסטיקה תשתיות ומערכות מידע) יפעל על פי השיקולים התפעוליים הארגוניים.

3.7.1. ראש אגף מחשוב ומערכות מידע אחראי על יישום מדיניות הגנת המידע בכללית, הוראות עבודה להגנת מידע מטעם הממונה על הגנת המידע בכללית, במערכות המידע ומערכות משובצות מחשב לרבות רכיבי תקשורת וציוד ומכשור רפואי (מותנה בנאמר בסעיף 5.14).

3.7.2. ראש אגף מחשוב ומערכות מידע יקבע כלים וטכנולוגיית הגנת מידע.

3.7.3. ראש אגף מחשוב ומערכות מידע יכתוב נהלי אבטחת מידע לגורמים המיישמים, את הגנת המידע, שבאחריותו.

3.7.4. ראש אגף מחשוב ומערכות מידע יבקר את נושאי הגנת המידע שבאחריותו.

3.7.5. ראש אגף מחשוב ומערכות מידע יתחזק את תקן ISO27799 באגף מחשוב ומערכות מידע.

3.8. **<u>מנהל ביטחון ארצי</u>**

3.8.1. מנהל ביטחון ארצי אחראי על יישום בקשות אבטחה פיזית וקביעת כלי אבטחה פיזיים על המידע, טיפול בעבירות הגנת מידע וביצוע ביקורת על הנושאים שבאחריותו.

3.9. **<u>סמנכ"ל וראש חטיבת משאבי אנוש</u>**

3.9.1. סמנכ"ל וראש חטיבת משאבי אנוש אחראי על ביצוע הדרכת והכשרת עובדים, רישום ההדרכות בתיקו האישי של העובד במסגרת "כישור הליבה" של נושא הגנת המידע.

3.9.2. סמנכ"ל וראש חטיבת משאבי אנוש יוודא שיפור מתמיד של רמת מודעות העובדים להגנת מידע במסגרת "כישור ליבה".

3.9.3. סמנכ"ל וראש חטיבת משאבי אנוש יוודא שכל עובד, מכל תצורת העסקה, הנקלט בכללית או עוזב את הכללית ייקלט/יגרע ממערכת SAPHR כ"**משתמש פנימי**".

3.9.4. סמנכ"ל וראש חטיבת משאבי אנוש יוודא שכל עובד, מכל תצורת העסקה, הנקלט בכללית יבצע מבחן אמינות. בנוסף תבוצע שיחה ותיעוד של ממליצי המועמד.

3.10. **<u>נאמן הגנת מידע מוסדי</u>**

3.10.1. בכל מוסד/מחוז/בית חולים/חברת בת, ימונה מנהל בכיר, בעל כישורים מתאימים, כמרכז את נושא הגנת המידע באותו מוסד. הנאמן המוסדי יקבל כתב מינוי ממנהל המוסד ויוכשר לנושא על ידי הממונה על הגנת המידע בכללית.

3.11. **<u>נאמן הגנת מידע מקומי</u>**

3.11.1. בכל יחידה/מחלקה בבי"ח/מרפאה/שלוחות של שירותי בריאות כללית בבתי"ח ציבוריים (להלן מתקן), ימונה נאמן הגנת מידע, בנוסף לתפקידו העיקרי.

3.11.2. נאמן הגנת המידע יוודא קיום נוהלי הגנת המידע במתקן אליה הוא שייך, תוך תיאום ודיווח מקצועי לנאמן הגנת המידע במוסד שלו ולממונה על הגנת המידע בכללית וזאת בכדי למנוע הגעת מידע "חסוי אישי" לגורמים בלתי מוסמכים.

3.11.3. מינוי הנאמן ייעשה על ידי נאמן הגנת המידע המוסדי בתאום עם מנהל המתקן בכתב ובכפוף להכשרה שתקבע על ידי הממונה על הגנת המידע בכללית.

3.11.4. בהעדר נאמן הגנת מידע, האחריות תהיה על מנהל המתקן או המנהל האדמיניסטרטיבי של המתקן. ברמת המנהלת בקהילה, תחול האחריות על המנהל האדמיניסטרטיבי של המנהלת.

3.12. **<u>המנהל האדמיניסטרטיבי</u>**

3.12.1. המנהל האדמיניסטרטיבי בכל מתקן אחראי על וידוא פעולת נאמן הגנת המידע בתוך אותו מתקן או יחידה ארגונית קטנה, אליה הוא שייך או עליה הוא אחראי במסגרת תפקידיו.

3.13. **<u>בעל הנכס/בעל המידע/משתמש בנכס</u>**

3.13.1. לכל מידע ומערכת מידע, חוצת ארגון או מקומית, ימונה בעל נכס בהתאמה.

3.13.2. בעל הנכס אחראי על סיווג המידע ושילוב דרישות ובקרה של הגנת המידע לפי המדיניות לכל משך מחזור החיים של המערכת.

3.13.3. בעל הנכס יקבל הכשרה והדרכה מתאימים, על פי הנחיית הממונה על הגנת המידע בכללית.

3.13.4. בעל הנכס אחראי על ניהול ובקרת ההרשאות במערכת שבאחריותו.

3.13.5. משתמש בנכס/בעל הסיכון יונחה על ידי בעל הנכס כיצד להשתמש בנכס.

3.14. **<u>וועדת הרשאות</u>**

3.14.1. לכל מערכת מידע קלינית/ עסקית חוצת ארגון תוקם וועדת הרשאות. בראשות הוועדה יעמוד רפרנט המערכת שהוא הלקוח העסקי של המערכת בהנהלה הראשית. הממונה על הגנת המידע בכללית הינו אחד מחברי הוועדה. אחריות מינוי יו"ר הוועדה הינה באחריות הסמנכ"ל, שבתחומו הפעלת השירות לו נחוצה המערכת.

3.14.2. וועדת ההרשאות תקבע את הכללים להקצאת הרשאות במערכת בהתאם למדיניות זו ובחתך סוגי המידע ובעלי התפקידים שרשאים לקבל גישה למערכת בשילוב עקרון הפרדת תפקידים. ותקבע בהתאם לכך פרופילים של הרשאות שישמשו בסיס לניהול ההרשאות במערכת.

3.14.3. אישור להרשאה חריגה, מפרופיל ההרשאות שנקבע, יינתן באישור וועדת הרשאות חריגות בראשות הממונה על הגנת המידע בכללית.

3.15. **<u>אחריות רישום מאגרי מידע</u>**

3.15.1. רישום מאגרי מידע, על פי הגדרתם להלן, כמתחייב מחוקי המדינה, הינו באחריות מנהל המוסד האחראי על המערכת הכוללת את מאגר המידע. ביצוע הרישום ברמו"ט (רשות למשפט וטכנולוגיות מידע במשרד המשפטים) הוא באחריות מנהל הכספים במוסד. מעקב הרישום, עדכון מאגרי המידע ותשלום האגרה השנתית ינוהל ע"י הממונה על הגנת המידע בכללית.

3.15.2. ראש אגף מחשוב ומערכות מידע או מנהל מחשוב מוסדי יודיעו לממונה הגנת מידע על הפסקת פעולתו של מאגר מידע שבאחריותו. ממונה הגנת המידע יודיע לרמו"ט על הפסקת פעילות המאגר.

4. הגדרות ומונחים

4.1. **מידע** – מידע מכל סוג, לרבות מידע כתוב, רשומות ומסמכים, מידע אלקטרוני, מידע קולי, מידע חזותי, שמעובד, משונע, או מאוחסן בכללית. לצורך סעיף זה:

4.1.1. מידע כתוב – מידע כתוב או מודפס על גבי מצע שאינו מצע אלקטרוני.

4.1.2. רשומות ומסמכים - כל אמצעי עליו ניתן לשמור או להציג מידע.

4.1.3. מידע אלקטרוני – מידע המופק במערכות משובצות מחשב ומוצג באמצעים אלקטרוניים או מועבר בתקשורת אלקטרונית, לרבות מידע במחשוב וציוד רפואי

4.1.4. מידע קולי – מידע המועבר באמצעות קולו של אדם במערכת מידע או מכונה אלקטרונית המייצרת קול.

4.1.5. מידע חזותי – מידע שנקלט בעין, לרבות מקום בו נראה מידע שיש בו כדי לזהות אדם פלוני.

4.2. **בעל ענין** – כל גורם פנימי או חיצוני אשר לו גישה למידע "חסוי אישי" או "חסוי" של הכללית. (מוסדות המדינה, חברות ביטוח, חברות מחקר)

4.3. **בעל נכס/בעל מידע** – גורם הנהלה המאשר לאחרים שימוש במערכת מידע או שינויים . (רפרנט)

4.4. **בעל הסיכון** – משתמש הקצה שמפעיל מערכת בהרשאה

4.5. **מנהל סיכון** – ראש חטיבה בהנהלה ראשית או מנהל מוסד אשר אצלו פועל המערכת כמערכת מקומית

4.6. **סיווג המידע** – קביעת רמת רגישות המידע, בהתבסס על העקרונות המפורטים במדיניות זו ומתוקף כל חוק ותקנה שחלים על המידע. סיווג המידע משמש כבסיס לקביעת רמת ההגנה הנדרשת.

4.7. **מידע רגיש** – על פי חוק הגנת הפרטיות התשמ"א 1981

4.7.1. נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו.

4.7.2. מידע ששר המשפטים קבע בצו, באישור וועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש.

4.8. **חסוי אישי** – רמת רגישות שהיא, כל פרט מידע או תהליך ממנו ניתן לזהות אדם פלוני ו/או מידע רגיש כהגדרתו בחוק הגנת הפרטיות התשמ"א – 1981.

4.9. **חסוי עסקי** – רמת רגישות שהיא, כל פרטי מידע או תהליך שיש בו מידע שאינו מידע רפואי ממנו ניתן לזהות פרטי אדם פלוני.

4.10. **בלתי מסווג** – רמת רגישות שהיא, כל פרט מידע שאין בו פרטים של אדם פלוני ואין בו מידע עסקי והוא כזה שאושר וניתן לפרסמו ברבים.

4.11. **הגנת מידע** – מהלך או פעולה כוללת של הגנה על המידע בארגון כך שיהיה:

אמין - מידע שלא נעשה בו שינוי מרגע שמחברו סיים כתיבתו או הפקתו.

זמין – המידע נגיש לבעלי תפקידים מתאימים ע"פ צרכי הארגון.

חסוי – מידע שתוכנו לא ייחשף לגורמים בלתי מוסמכים.

מבוקר – מידע עליו מופעלים תהליכים וכלי בקרה במטרה לוודא פעולה תקינה של שימוש במידע והגנת המידע לאורך כל נתיב המידע.

4.12. **נתיב המידע** – מעבר המידע בארגון בכל מקום ובכל דרך בה המידע נגלה לאדם שאינו המטופל עצמו. כך גם לגבי מידע עסקי שעובר בארגון ומחוצה לו מרגע שעזב את מחברו.

4.13. **אבטחת מידע** – יישום הגנת המידע בטכנולוגיות שבשימוש הכללית.

4.14. **שילוב הגנת מידע** – שילוב נהלים תהליכים ופתרונות טכנולוגיים שמטרתם הגנת מידע.

4.15. **מנהל בארגון** – כל עובד אליו כפופים עובדים.

4.16. **נאמני הגנת מידע** – בעל תפקיד, שבנוסף לתפקידו אחראי על הגנת המידע במוסד במרפאה/ מחלקה/ יחידה.

4.17. **תהליך** – סוג של פעולה ראשונית או פרויקט בתחום: מחשוב, משאבי אנוש, תכנון וארגון, לוגיסטיקה, בינוי תשתיות, ציוד/מכשור רפואי, שבהם עשוי להימצא מידע. כך גם לגבי עדכון גרסה, הכנסת שינויים במערכות, או שיפוץ מבנים.

4.18. **הרשאה** – אישור עקרוני ליצור ו/או לצפות ו/או לשנות סוג מסוים של מידע.

4.19. **סוג הרשאה** – הרשאת גישה למידע על פי פרופיל שנקבע לפי עיסוקו של העובד ותפקידו.

4.20. **צמתי מידע** – מרכז של מידע רב (רשת וחדרי מחשב, מח' רשומות, מערכות בעלות סגמנטים רבים, ארכיון וכיו"ב).

4.21. **ספק חיצוני** - כל אדם העובד בכללית או עבור הכללית ואינו עובד הארגון המחויב בתנאי העבודה בארגון (יחסי עובד-מעסיק).

4.22. **תקלה/פגיעה בהגנת מידע** – מצב בו נפגע חיסיון המידע, שלמות המידע, זמינות המידע, וכתוצאה מכך המידע הגיע לבלתי מוסמכים או נפגעה זמינותו ופגעה בשירות לקוחות או חיי אדם.

4.23. **פיתוח מאובטח** – פיתוח אפליקציית מחשב בה שולבו דרישות הגנת המידע ייחודית לשפת הפיתוח, כך שהמערכת תעמוד בדרישות ההגנה על המידע, בהתאם למדיניות זו.

4.24. **הלבנה/התאמה** – מצב בו עוברת תוכנה/חומרה/מידע בדיקת הגנת מידע בכללית ושולב בה כלי הגנה כדי לקיים את מדיניות הגנת המידע בכללית.

4.25. **<u>שינוי גרסה משמעותי</u>** – גרסה הגורמת לשינוי מהותי בתהליכי העבודה במערכת ו/או בממשק עם מערכות שלא היה להן ממשק עד כה, ו/או שיש שינוי באופן הקישור לאינטרנט, ו/או שינוי בהגדרות/מנגנוני אבטחת מידע ו/או שונו בה חוקי הזדהות והרשאות משתמשים, מנהלי מערכת ואנשי תמיכה.

4.26. **<u>ארוע הגנת מידע משמעותי</u>** – מצב בו נפגעה **זמינות, אמינות וסודיות** המידע ופגיעה בבקרה על המידע (למשל פגיעה בשלמות המידע, הדבקה בוירוסים לסוגיהם, גנבת מידע, או שיבוש מידע של לקוח, פגיעת גורם זר במידע או במערכת מידע של הכללית) בלמעלה מ-50 תחנות עבודה ו/או בלמעלה מ-5 מכשירים רפואיים יחד וכל אלו נמשכו מעל 60 דקות רצופות.

4.27. **<u>הזדהות חזקה חד ערכית</u>** – תהליך הזדהות הדורש סיסמה חזקה ואימות זהות ביומטרי של המשתמש.

4.28. **<u>נוזקת מחשב (Malware)</u>** – תוכנת מחשב שחודרת למחשב ללא ידיעת המשתמש, וגורמת על פי רוב לשיבושים ולתקלות שונות בהפעלת המחשב. התוכנה עוברת ממחשב למחשב ומריצה פקודות מחשב זדוניות עד כדי השתלטות מלאה על המחשב ללא ידיעת המשתמש. דוגמאות לשמות של נוזקה: וירוס, תולעת, סוס טרויאני.

4.29. **<u>הצפנה</u>** – תהליך מתמטי מחשובי הגורם לשינוי המידע מגלוי ומובן, לבלתי מובן לאלו שאינם מורשים לצפות במידע. תהליך ההצפנה מבוצע באמצעות תוכנה ייעודית אותה מפעילים גורמי המחשוב בארגון. מידע "חסוי אישי", שנחוץ להוציאו ממערכת המידע בכללית ולהעבירו להתקן חיצוני, יוצפן ע"ג ההתקן הנייד (דיסק און קי מוצפן, הצפנה במחשב נייד).

4.30. **<u>סייבר (Cyberx)</u>** – מרחב קיברנטי המורכב מתשתית תקשורת, מערכות מידע, ובני אדם המפעילים את המידע במרחב הקיברנטי.

4.31. **<u>עקרון הפרדת תפקידים</u>** – מהלך המוודא כי בעל הרשאה לא יוכל לבצע פעולה של שינוי מידע רפואי, או הפקת מידע רפואי, או גישה לבסיס נתונים, או פעולה כספית ללא שגורם נוסף אישר את הפעולה (על משקל "לא ישמור החתול על החלב").

4.32. **<u>וועדת הרשאות חריגות</u>** – וועדה בראשות הממונה על הגנת המידע בכללית, שדנה בבקשות להרשאות חריגות שאינן בפרופיל ההרשאות שנקבע במערכת.

4.33. **<u>רפרנט מערכת/לקוח עסקי/בעל מידע</u>** – מנהל מערכת מידע או תהליך שהזמין את המערכת או יזם את התהליך לשם הפעלת הפעילות או התהליך בכללית. לקוח עסקי הינו מטעם המוסד (מוסדות/הנהלה הראשית) ואינו איש מחשוב (אלא אם המערכת משרתת את גורמי המחשוב לצורך פעילותם הטכנית) במערכות ארגוניות.

4.34. **<u>אישור מראש ובכתב</u>** – לקוח או עובד אישר לכללית מראש ובכתב לשלוח לו מידע, בנושאים שיש בהם "מידע רגיש", באמצעים מקוונים או בדואר רגיל. ניתן לקבל אישור

שכזה גם בפקס וגם בדואר אלקטרוני בתנאי שבוצע וידוא מלא שאכן השולח הוא האדם לגביו מתייחס המידע.

4.35. **<u>סיכון הגנת מידע</u>** – מצב בו עלולה להיפגע או **נפגעה אמינות, זמינות וסודיות** המידע.

4.36. תחנת קצה – תחנת המחשב של המשתמש בארגון או תחנת המחשב בציוד משובץ מערכת מידע (למשל ציוד ומכשור רפואי, מדפסת, מכונת צילום).

4.37. **<u>נכס מידע</u>** – מקום או מכשיר אלקטרוני בהם יש מידע "חסוי אישי"/"חסוי עסקי" של למעלה מ 500 בני אדם.

4.38. **<u>מוסדות הכללית</u>** – בתי חולים, מחוזות הקהילה, מנהל אספקה, מעבדה מרכזית, מערך ביטוח מושלם, ההנהלה הראשית.

4.39. **<u>מאגר מידע</u>** – כל מערכת מידע שמאחסנת בבסיס הנתונים שלה מידע על 500 בני אדם לפחות.

4.40. **<u>משתמש פנימי</u>** – עובד שנקלט במערכת ניהול משאבי אנוש SAPHR.

4.41. **<u>משתמש חיצוני</u>** – עובד שנפתח לו חשבון משתמש אך לא נקלט במערכת ניהול משאבי אנוש SAPHR.

4.42. **<u>חברות בנות/חברות הבת</u>** – ש.ל.ה, מור, כללית הנדסה רפואית.

5. <u>עקרונות הגנת המידע בכללית</u>

5.1. מידע ותהליכים המעבדים את המידע או מאחסנים אותו, יאובטחו על פי מדיניות זו בכל עת ובכל מקום בו הם נמצאים ו/או אמורים להימצא בשליטה ובבעלות הכללית וחברות הבנות או אצל בעלי ענין חיצוניים.

5.2. מידע ומערכות המעבדות או מאחסנות אותו, לרבות ציוד ומכשור רפואי, הנמצאים בתחומי הארגון, או שנמסרו לספק חיצוני לצורך מתן שרות לארגון, הם רכוש הארגון וכפופים למדיניות זו.

5.3. מידע ישמר באופן שיהיה **<u>זמין, אמין, סודי ומבוקר</u>** ע"פ הנדרש לקיום מטרות ויעדי הכללית.

5.4. כל ייזום מאושר של תהליך בארגון, תהליך או"ש או תהליך בו משולבת מערכת מידע ובינוי ויש בתהליך מידע "חסוי אישי" או "חסוי עסקי", תשולב דעתו המקצועית של הממונה על הגנת המידע בכללית. בשלב האפיון של התהליך, ישולבו דרישות הגנת מידע מטעם הממונה על הגנת המידע בכללית. האחריות לשילוב הדרישות הינה על יוזם התהליך. במערכות מידע- האחריות של ראש אגף מחשוב ומערכות מידע להודיע לממונה הגנת המידע על כל ייזום שאושר.

5.5. ניהול סיכוני הגנת מידע – יבוצע תהליך רציף של ניהול סיכוני הגנת מידע, לרבות סקר סיכונים והערכת סיכונים. ניהול הסיכונים יבוצע, בין היתר, באמצעות מערכת ניהול סיכוני הגנת מידע באחריות הממונה על הגנת המידע בכללית.

5.6. מדיניות קבלת סיכונים:

5.6.1. ההנהלה תנהל את אבטחת המידע לפי סקר הסיכונים וטבלאות ניהול הסיכונים הנובעים ממנו.

5.6.2. בכל סיכון ברמה 20-25 הנחשב סיכון גבוה בהגדרתו על ידי החברה, ינקטו בקרות וצעדים הנדרשים להקטנת הסיכון בפרק זמן שלא יעלה על 4 חודשים, למעט בקרות הנדרשות לתקציבים גדולים ושינוים מערכתיים.

5.6.3. במקרים חריגים מסוג זה תאשר ההנהלה בקרות מפצות ככל שניתן ותקציב וזמן כנדרש לסגירת הסיכון.

5.7. גישה למידע תהיה מותנית בהרשאות מתאימות הנגזרות מהתפקיד, על פי הנחיצות למילוי התפקיד ובאישור הלקוח העיסקי המופקד על מערכת המידע. פרופיל ההרשאות יובא לאישור הממונה על הגנת המידע בכללית (מנהל ההרשאות הארגוני).

5.8. מדיניות זו כפופה ומבוססת על הוראות הדין (לרבות חוקים, תקנות ונהלים) אשר עניינם בהגנה על מידע ובכלל זה, אך מבלי לגרוע מכלליות האמור, חוק הגנת הפרטיות, חוק המחשבים, חוק זכויות החולה, תקנות בריאות, חוזרי ונהלי משרד הבריאות, חוק יסוד כבוד האדם וחירותו וכיו"ב. וכן חוזר מנכ"ל משרד הבריאות מס' 3/2015 המחייב את ארגוני הבריאות והספקים עמה היא קשורה, בעמידה בדרישות אבטחת מידע ותקן אבטחת מידע למערכות בריאות, ISO27799.

5.9. מדיניות זו תתורגם, על ידי הממונה על הגנת המידע בכללית, להוראות עבודה להגנת מידע הלכה למעשה. אלו יהוו קווים מנחים לביצוע הגנת המידע בידי הגורמים המיישמים את הגנת המידע, ובפרט, ראש אגף מיחשוב ומערכות מידע ומנהלי המחשוב במוסדות, אשר ייקבעו הוראות עבודה בתחומם, הכול בהתאם למדיניות וסעיף 5.14 וסעיף 3.6.3 כאמור.

5.10. בכל תהליכי העבודה בארגון בהם יש מידע "**חסוי אישי**"/"**חסוי עסקי**" ישולבו דרישות הגנת מידע. שילוב הדרישות יבוצע כבר בשלב האיפיון של התהליך. בשלב הייזום של התהליך תשולב דעתו של הממונה על הגנת המידע בכללית. אחריות על שילוב הדרישות חלה על יוזם התהליך. **<u>במקרה של מערכות מידע</u>** – א. יודיע ראש אגף מחשוב ומערכות מידע לממונה על הגנת המידע, רק על הייזומים שיאושרו. ב. שילוב דרישות הגנת המידע בתהליך האפיון הוא האחריות מנהל הפרויקט באגף מחשוב ומערכות מידע ומנהלי מחשוב במוסדות וחברות הבת.

5.11. לא ישולבו למערכות המידע של הארגון או בבעלות הארגון כל סוג מידע, חומרה, תוכנה, מכשור רפואי אלא אם עברו בדיקת הלבנה/התאמה של הגנת מידע ונתקבל לכך אישור מטעם הממונה על הגנת המידע בכללית. ובכפוף לסעיף 5.14 להלן

5.12. קיום מדיניות זאת והוראות העבודה שנקבעו מכוחה הוא תנאי יסודי להמשך העסקתו של כל עובד והפרתו תטופל משמעתית ועל פי החוק.

5.13. כל שינוי או חריגה מהאמור במדיניות זו או שינוי ביישום/הגדרות הגנת מידע דורש אישור מראש מטעם הממונה על הגנת המידע בכללית ובכפוף לנאמר בסעיף 3.6.3 לעיל . הממונה על הגנת המידע בכללית יודיע על כל שינוי כאמור לסמנכ"ל וראש חטיבת לוגיסטיקה תשתיות ומערכות מידע.

5.14. תקציב יישום הגנת המידע הינו תקציב ייעודי שמוקצה על ידי הנהלת הכללית. יישום מרכיבי אבטחת מידע ייחודיים למערכת מידע ושינוי גרסה יבוצע מתקציב הפיתוח של מערכת המידע.

5.15. מדיניות הגנת המידע הינו מסמך יסוד בו משולבת תורת הגנת המידע בכללית. יישומה במערכות המידע דורש תקציבים כבדים . כדי ליישמה בתבונה ובאילוצי התקציב השנתי, תתוכנן תוכנית עבודה שנתית, בשיתוף ראש אגף מחשוב ומערכות מידע והממונה על הגנת המידע. מידי שנה בחודש אוקטובר, תובא התוכנית לאישור סמנכ"ל וראש חטיבת לוגיסטיקה תשתיות ומערכות מידע.

5.16. תוכנית העבודה השנתית תצביע על שיפור ברמת הגנת המידע בכללית בהשוואה לשנה הקודמת. תוכנית העבודה השנתית תתוכנן כך שתתן מענה לצמצום סיכוני הגנת המידע שנקבעו באסטרטגיית הגנת המידע בכללית או כמענה לאיומי הגנת מידע חדשים.

5.17. שירותי בריאות כללית תפעל לקיום דרישות תקן ISO27799 בכל מוסדותיה וחברות הבת. כמו גם קיום הגנת הפרטיות בדרישות האקרדיטציה.

5.18. חל איסור להוציא/לשלוח מהכללית מידע "חסוי אישי" באמצעות האינטרנט, הדואר האלקטרוני, אמצעים מקוונים, אלא אם התקיימו תנאים אלה:

5.18.1. המטופל אישר זאת מראש ובכתב,

או

5.18.2. התקבל אישור מטעם הממונה על הגנת המידע בכללית.

5.19. שירותי "ענן" (cloud) – חל איסור להעברת מידע "חסוי"/"חסוי אישי" לשירותי ענן. אלא אם המידע מוצפן/מעורבל ואלגוריתם ההצפנה/הערבול נשאר בידי הכללית.

5.20. לכל משתמש במערכת מידע לרבות אנשי מחשוב תוקצה סיסמה ושם משתמש אישי. חל איסור שימוש בשם משתמש וסיסמה כלליים (מרובי משתמשים).

5.21. הרשאת משתמש שלא בוצע בה שימוש מעל 90 יום תינעל כך שהפעלה מחדש דורשת אישור מטעם הלקוח העסקי/רפרנט המערכת ובאישור הממונה על הגנת המידע בכללית או אישור מנב"ט מוסדי אליו שייך העובד.

5.22. לכל מידע "חסוי אישי"/"חסוי" והדואר האלקטרוני יבוצע תהליך גיבוי. אחת לחצי שנה יבדק מדגמית שחזור הגיבוי.

5.23. כל סוג של גישה למידע "חסוי אישי" לגורמים שאינם צוות רפואי מחייב אישור יו"ר הוועדה אתיקה עליונה להגנת מידע (לא כולל אנשי מחשוב).

5.24. הזדהות משתמש לכל מערכת מידע לרבות ציוד ומכשור רפואי תבוצע באמצעות שרת אימות מרכזי (AD).

5.25. חל איסור שימוש בתוכנה מכל סוג אלא אם נרכשה או שימוש בה נעשה כנדרש בחוק ומאושרת על ידי הממונה על הגנת המידע בכללית.

5.26. כל שימוש במחשב ייעשה על פי המתחייב מחוק המחשבים התשנ"ה 1995.

6. <u>סיווג וסימון רגישות המידע</u>

6.1. כל רשומה, מסמך, מערכת או תהליך המכילים, מעבדים או מעבירים מידע יסווגו ברמת רגישות ויאובטחו בהתאם לדרישות הגנת המידע הנגזרות מהסיווג.

6.2. **<u>רגישות וסיווג מידע</u>** - המידע בארגון הינו מסוגים שונים, כגון מידע רפואי אישי של מטופל, מידע רפואי כללי שאינו מזהה מטופל, מידע עסקי, מידע פיננסי, מידע אישי המתייחס לעובד, מידע פרסומי ומידע אחר. כל יחידת מידע תקוטלג לאחת מרמות סיווג הרגישות הבאות:

6.2.1. **<u>חסוי אישי</u>** - כל מידע שעשוי לחשוף את פרטיו הרפואיים, או נתוני כ"א ושכר, של אדם פלוני (כמוגדר בחוק הגנת הפרטיות התשמ"א 1981). מידע זה יוגן על פי החוק ובכל האמצעים הסבירים כדי שלא ייחשף לבלתי מורשים.

6.2.2. **<u>חסוי עסקי</u>** - כל מידע בו נתונים פיננסיים, מידע רפואי כללי, מחקרים רפואיים, מידע עסקי, מידע סטטיסטי וכל מידע שאין הכללית חייבת לחשוף על פי האמור בחוק חופש המידע. גם מידע אחר שחשיפתו לבלתי מורשים או פגיעה באמינותו או בזמינותו עלולים להביא נזק חמור לניהול התקין של הכללית, לתדמיתה, או לספק יתרון למתחרה ו/או כל מידע שפגיעה בזמינותו או באמינותו עלולה לגרום לנזק בגוף האדם.

6.2.3. **<u>לשימוש פנימי</u>** – מידע שנועד לצורך עבודה שוטפת והוא נגיש לכלל עובדי הארגון, על פי הצורך.

6.2.4. **<u>בלתי מסווג/לפרסום</u>** - מידע שנועד להיות מפורסם לציבור הרחב.

6.3. **<u>סיווג מערכות מידע</u>**

6.3.1. מערכות המידע והמכשור הרפואי בכללית יסווגו לאחת מרמות הקריטיות, בהתאם לדרישות הזמינות של המערכת:

א. **<u>מערכת רגילה</u>** – מערכת אשר גם אם תושבת למשך 7 ימי עבודה, לא ייגרם נזק או הפרעה משמעותיות לפעילות.

ב. **<u>מערכת חשובה</u>** – מערכת אשר אם תושבת למשך 2 ימי עבודה, ייגרם נזק ו/או הפרעה משתמעותית לפעילות.

ג. **<u>מערכת קריטית</u>** – מערכת אשר חייבת להיות זמינה בכל עת, ובמקרה של השבתה נדרשת התאוששות תוך 6 שעות.

ד. **<u>מערכת תומכת חיים</u>** – מערכת שהשבתה שלה עשויה לסכן חיי אדם.

6.4. **<u>סימון מידע</u>**

6.4.1. סיווג רמת הרגישות של המידע יצויין במקום בולט לעין – כך שעין אדם תוכל לראותו בנקל בטרם תחל לעיין במידע (דפי נייר, דפי מידע על גבי צג מחשב, ציוד וכיו"ב). הסיווג יצוין בראש כל דף במסמך, בכל מסך בו צופים במידע, ע"ג ציוד או מתקן שהוא המידע.

6.4.2. מסמך או מידע שלא מצוינת עליו רמת רגישות ייחשב כמסווג "לשימוש פנימי".

7. <u>שילוב בקרות הגנת מידע בארגון</u>

7.1. **<u>ניהול סיכוני הגנת מידע</u>**

7.1.1. רמת הגנת המידע בכללית מבוצעת ביחס לרמת הסיכון הנשקפת לפעילות ולמידע של הכללית כתוצאה מהשימוש במידע ובמערכות מידע. הממונה על הגנת המידע בכללית יבצע תהליך רצוף של ניהול סיכונים במגמה לצמצם סיכונים ככל שניתן.

7.1.2. יו"ר וועדת אתיקה עליונה להגנת המידע או הממונה על הגנת המידע בכללית יציג אחת לשנה להנהלת הכללית את מצב הגנת המידע בכללית. הצגת הנושא היא ביחס לנדרש במסמך מדיניות זה.

7.2. **<u>הגנה על מידע</u>**

7.2.1. הוצאת מידע המוגדר כחסוי (אישי או עסקי) מחוץ למתקני הכללית או ביניהם, מחייב התייחסות מחמירה מהנהוגה בתוך מתקני הכללית, כמפורט בנוהל מסירת מידע רגיש בכללית 08-01-02 והוראות העבודה להגנת מידע הרלבנטיות.

7.2.2. אין לפרסם או לשתף בכל דרך שהיא מידע, לרבות תמונות, אשר יש בהם כדי לחשוף מידע של הכללית, ובפרט מידע חסוי אישי. כל פרסום מידע כאמור מחייב אישור מראש של הממונה על הגנת המידע בכללית ודוברת שירותי בריאות כללית.

7.2.3. בשל רגישותו, מידע "חסוי אישי" יוגן באמצעות הצפנה ובאמצעי בקרת גישה מחמירים. בעת הוצאת מידע "חסוי אישי" כאמור יינקטו הצעדים הנאותים בכדי להבטיח שפרטיות ומהימנות המידע יישמרו. לצורך כך יופעלו אמצעי הגנה שונים, לרבות אמצעי בקרת גישה ברמת הקובץ.

7.2.4. הפקה של דו"חות בהם מצוי מידע "חסוי אישי"/"חסוי עסקי" דורשת התייחסות מחמירה באמצעות הרשאות מתאימות או באישור הממונה על הגנת המידע בכללית.

7.2.5. עובד לא ימסור מידע "חסוי אישי" לאדם, לרבות לעובד אחר, בטרם וידא, באופן מושלם את זהותו של מקבל המידע ואת הצורך שלשמו נמסר המידע. באם הגיע לעובד מידע "חסוי אישי" שלא במסגרת תפקידו, או שנודע לו על מסירת מידע כאמור, יעביר על כך דיווח למנהלו הישיר, המנהל הישיר יעביר דיווח לנאמן הגנת מידע מוסדי ולממונה על הגנת המידע בכללית.

7.2.6. מסירת המידע לאדם תתבצע באופן המבטיח את פרטיות המידע. בפרט, במקומות בהם ניתן שירות לקהל, שם יישמר מידור בין מקבל המידע או השירות לבין כל גורם אחר. בחדרי אשפוז בהם יש מאושפזים נוספים יוודא הצוות הרפואי את שמירת פרטיות האדם ככל שניתן.

7.2.7. מחשב של שירותי בריאות כללית, המחובר לרשת הכללית ו/או מכיל מידע "חסוי אישי", הנמצא ליד מיטת חולה או מטופל, לא יישאר ללא השגחה של איש צוות, ובאם יושאר ללא השגחה כאמור, יש לצאת מהמערכת עליה עבד איש הצוות ולבצע log off כך שפעולה במחשב תחייב סיסמת גישה.

7.2.8. כל סוג של נייר (להוציא נייר טואלט ונייר סדין מיטה, כיסוי מיטה, ניגוב ידיים) או רכיב זיכרון או מידע רפואי הנמצא על גבי מצע פלסטי יושמד רק בדרך של גריסת פתיתים. רכיב זיכרון יכול להיות מושמד גם בדרך של מיגנוט המסיר את המידע כך שלא ניתן לשחזרו. רכיב זיכרון תקול או להחלפה לא ייצא את גבולות הכללית ללא שבוצע בו תהליך מגנוט או ניקוב כך שלא ניתן יהיה לשחזר את המידע בו.

7.3. **<u>הגנת מידע בתרבות הארגונית</u>**

7.3.1. הגנת המידע הינה **"כישור ליבה"** לכל העובדים בכללית וחברות הבת.

7.3.2. ככלל, עובדי הכללית יקבלו הדרכת הגנת מידע נאותה, בהתאם לדרישות התפקיד ו"כישור הליבה" עליו הוחלט. כל עובד הכללית יעבור הדרכת הגנת מידע בכניסתו לעבודה בכללית ואחת לשלוש שנים לכל הפחות.

7.3.3. עובד חדש או עובד של ספק חיצוני, בתהליך קליטתו או העסקתו, יקבל הדרכת הגנת מידע ויחתום על התחייבות לשמירת סודיות והגנת מידע על פי מדיניות הגנת המידע ונוהלי העבודה בארגון. ההדרכה וההחתמה באחריות נציג מחלקת משאבי אנוש הקולט את העובד.

7.3.4. הגנת מידע תשולב בכל מסגרות ההכשרה במחלקת הדרכה ובכל מסגרות הכשרה מטעם החטיבות בהנהלה הראשית ובבתי הספר לסיעוד, או גופים המעבירים הכשרה/לימודים לעובדי הכללית. בפרט, בכל חוברת הדרכה או ערכת הדרכה, לרבות ערכות מתוקשבות ולומדות, ישולב פרק הנחיות הגנת מידע.

7.3.5. כל אדם העוסק בפיתוח מערכות מידע יוכשר בנושא הגנת המידע כדי שבעת עבודת הפיתוח יפעל לפי תורת "פיתוח מאובטח".

7.3.6. כל אדם העוסק בתקשורת ותכנון תשתיות יוכשר בנושא הגנת המידע לשם תכנון תשתיות ותקשורת מאובטחת.

7.3.7. כל ביצוע הדרכה/הכשרה של עובד, בדגש על "כישור ליבה", יתועד בתיקו האישי של העובד.

7.4. **<u>ציוד ומכשור רפואי משובץ מחשב</u>**

7.4.1. רכיבי ציוד ומכשור רפואי, הכוללים מידע "חסוי אישי", שנוצר ו/או שמעובד ו/או שמאוחסן ו/או שמועבר דרכם, חייבים לעמוד בסטנדרטים מתאימים להגנת המידע ושמירה על הפרטיות, על פי מדיניות זו והוראות עבודה מתאימות מטעם הממונה על הגנת המידע בכללית.

7.4.2. ככלל, מערכות מחשב וציוד רפואי לא יחזיקו מידע "עודף", דהיינו, מידע אשר אינו נחוץ לצורך השימוש בהן.

7.4.3. במערכות מחשוב וציוד ומכשור רפואי לא ייעשה שימוש בתווך אלחוטי, אלא בכפוף לאישור הממונה להגנת המידע בשיתוף אגף מחשוב ומערכות מידע.

7.4.4. כל ציוד ומכשור רפואי שהופסקה פעילותו, בכללית לרבות סיום תהליך הערכה/ניסוי, יוסר ממנו מידע "חסוי אישי" באופן שלא ניתן לשחזרו. הסרת המידע הינה באחריות הגורם שהחליט להפסיק את הפעילות או ריכז את תהליך הערכה/ניסוי.

7.5. **<u>מהימנות כ"א</u>**

7.5.1. עובדים בצמתי המידע יאושרו למילוי תפקיד רק לאחר אישור מהימנות מתאים מטעם מנהל ביטחון ארצי/ מנהל ביטחון מחוזי/ מוסדי/ בית חולים/ חברת בת.

7.5.2. עובדי חברות יעוץ חיצוני/ ספקים וגורמים חיצוניים העובדים בכללית או עבור הכללית ולהם יש גישה למידע שיש בו פרטים של אדם פלוני המסווג "חסוי אישי"/ "חסוי עסקי" יידרשו לאישור אמינות מטעם חברת מיון כ"א. אישור האמינות יהיה

מטעם קצין ביטחון בליווי תוצאות מבחן אמינות של חברת מיון כ"א מטעם הספק או מי מטעמה. במקרים חריגים יידרש אישור מטעם מנהל ביטחון ארצי, או בא כוחו, טרם תחילת העסקתם.

7.5.3. כתנאי לקליטת עובד מחשוב, לכל תפקיד, נדרש להמציא אישור ביצוע מבחן אמינות ואישור גורם ביטחון המאשר את אמינות העובד. ביצוע התהליך הינו באחריות הספק החיצוני טרם קליטת העובד.

7.5.4. עובד מחשוב, מכל סקטור, העובד בכללית ומשנה תפקידו בכללית יידרש לבצע מבחן אמינות על פי האמור בסעיף 7.5.3 לעיל (במקרה זה ניתן לבצע את מבחן האמינות באמצעות מנהל ביטחון ארצי/מוסדי).

7.6. **<u>עבודה מול גורמים חיצוניים</u>**

7.6.1. ככלל, כל מתן גישה למידע (מכל סוג) או למערכות מידע או למערכות רפואיות של הכללית (לרבות חברות בת), בין אם בדרך של קישור מערכות מחשב, משלוח קבצים או מדיות, או בכל דרך אחרת, מחייב אישורים בסטנדרטים שיקבעו על ידי הממונה על הגנת המידע בכללית ואגף מחשוב ומערכות מידע.

7.6.2. גורם חיצוני לא יקבל גישה למידע פנימי או חסוי של הכללית אלא בכפוף לחתימה על הסכם שמירת סודיות והגנת מידע והסכמה לביצוע הנחיות הגנת המידע של הכללית.

7.6.3. בכל חוזה התקשרות עם ספק/גורם חוץ או מכרז, שבשירות המבוקש יש לספק או עובדיו חשיפה/גישה למידע של בני אדם, או שהכללית מעבירה לספק מידע או שעובדי הספק נמצאים, ואפילו זמנית, במתקני הכללית, ישולב פרק הגנת מידע. האחריות לשילוב פרק הגנת מידע חלה על יוזם חוזה ההתקשרות/מכרז. הממונה על הגנת המידע בכללית יפרסם, מעת לעת, הנחיות פרטניות בנושא זה.

7.6.4. אחת לשנה תבוצע, על ידי הממונה על הגנת המידע בכללית או מי מטעמו, ביקורת של ספקים המחוברים לכללית, או שנתנה להם גישה למידע חסוי, וזאת בכדי לוודא עמידתם בדרישות הגנת המידע.

7.6.5. כל הוצאת מידע מחוץ לארגון, לצורך ביצוע מחקר, מחייבת אישור מראש ובכתב של הוועדה להוצאת נתונים במשרד הרופא הראשי ופעילות בסטנדרט שנקבע במשותף עם הממונה על הגנת המידע בכללית. הוצאת מידע שיש בו לזהות פרטי אדם פלוני, מחייבת ערבול הנתונים באופן שלא ניתן יהיה לקשור בין פלוני למידע הרפואי שלו. במידת שיש צורך בכך, יכולת פענוח וקישור המידע לאדם פלוני תשמר בתוך שירותי בריאות כללית בלבד.

7.6.6. ספק חיצוני אשר לצורך ביצוע עבודתו חייב להיחשף למידע של הכללית המוגדר כחסוי (אישי או עסקי) יידרש כתנאי להעסקתו, לעמוד בכל דרישות הגנת המידע.

7.7. **<u>שימוש נאות</u>**

7.7.1. משאבי המחשוב והתקשורת של הכללית נועדו לסייע לעובדים למלא את משימותיהם בארגון. השימוש במשאבי הארגון לצרכים פרטיים, מכל סוג, אסור.

7.7.2. שילוב חומרה או תוכנה פרטית למערכות המידע אסור.

7.7.3. חל איסור לשלוח בדואר האלקטרוני הארגוני מסרים פרטיים מסוג: "מכתבי שרשרת", מסרים מטעם ארגונים, כתות, פרסומיים מסחריים שאינם לצרכי עבודה, מסרים שאינם הולמים ועשויים לפגוע בצנעת הפרט, מסרים שיש בהם דבר הסתה. מידע פרטי אחר לא יישלח בתפוצת פורומים/קבוצות אלא אם התקבל לכך אישור מראש מטעם הממונה על הגנת המידע בכללית או מנהל הפורום/קבוצה.

7.7.4. עובד לא יעשה שימוש במידע שהגיע אליו מכורח תפקידו למטרות פרטיות ו/או שאינן לצורך מילוי תפקידו.

7.7.5. אין להעלות מידע ארגוני פנימי או מידע של על עובד או מטופל או לקוח, מכל סוג, לאינטרנט אלא באישור דוברת שירותי בריאות כללית והממונה על הגנת המידע בכללית.

7.8. **<u>אבטחה פיזית</u>**

7.8.1. מתקנים בהם מאוחסן או מעובד מידע יוגנו באמצעי כנגד חדירה פיזית בלתי מורשית, גניבה, אש, הצפה וכדומה בכדי למנוע גישה בלתי מורשית, נזק ו/או הפרעה לפעילות.

7.8.2. מידע חסוי יישמר בארונות נעולים. ציוד ומערכות המכילות מידע חסוי יוצבו באזורים ייעודיים, והגישה אליהם תוגבל למורשים בלבד.

7.8.3. בכללית תונהג מדיניות "**שולחן נקי**" דהיינו, בסיום יום העבודה/משמרת ובכל מקרה בו עובד עוזב את סביבת עבודתו, תהיה סביבת העבודה נקיה ממידע רגיש ויינקטו מכלול הצעדים שיש ביכולתם למנוע גישה של זרים למידע: מערכות מחשב יינעלו באופן שגישה אליהן תחייב הזדהות, מידע כתוב, לרבות מדיות ומצעים מגנטיים, יינעל בארון, מידע שנועד לגריסה ירוכז במקום מאובטח שנועד לכך, דלתות המשרד יינעלו.

7.8.4. כל מערכת מידע המוצבת בשטח ציבורי תפוקח באמצעות מצלמת אבטחה.

7.8.5. פעולת תחזוקה של טכנאי חיצוני, שאינו עובד קבוע בכללית, מחייבת ליווי צמוד של איש צוות המתקן. לאחר שאיש הצוות וידא עם גורם מקצועי מתאים בהנהלת המוסד את הצורך בפעולת הטכנאי.

7.8.6. הוצאת ציוד מחשוב אל מחוץ למתקני הכללית מחייבת אישור של מנהל המחשוב במוסד.

7.8.7. "זיהוי וודאי" של אדם יבוצע על פי נוהל מסירת מידע רגיש מס' 08-01-02.

7.9. **<u>בקרת גישה</u>**

7.9.1. בקרה על ניהול המשתמשים וההרשאות בכללית הינו באחריות הממונה על הגנת המידע בכללית.

7.9.2. הרשאות למערכות המידע יינתנו תוך התחשבות בעיקרון הפרדת תפקידים.

7.9.3. הרשאות גישה יוענקו לבעלי תפקיד על פי הנחיצות בגישה למידע לשם מילוי התפקידים והמידור המתחייב מרגישות המידע. הרשאה תוענק על ידי רפרנט המערכת באישור יוצרי המידע ו/או וועדת האתיקה עליונה להגנת מידע בהנהלה הראשית.

7.9.4. לכל אדם בכללית ומחוץ לכללית מכל סקטור שהוא, לרבות חברות חיצוניות להם עובדים בכללית, תפתח רשומה במערכת כ"א, זו תשמש בסיס לפתיחת חשבון משתמש ברשת הכללית, ניהול זהויות ושיוך לתפקידים.

7.9.5. חשבון המשתמש יהיה ייחודי ויהיה בשימושו האישי של האדם לו הוקצה. שימוש במערכות המידע של הכללית מותנה בהזדהות אישית חד ערכית של המשתמש.

7.9.6. עבור חשבונות משתמש רגישים (מנהלי מערכות מידע ותשתיות תקשורת, תומכים טכניים כאלה שקיבלו הרשאות מועדפות וכיו"ב) נדרשת הזדהות חד ערכית, למעט באישור חריג ומראש של הממונה על הגנת המידע בכללית, בפרט, לא ייעשה כל שימוש בחשבונות גישה משותפים.

7.9.7. רשומת המשתמש ותפקידיו יעודכנו כך שישקפו בכל עת מצבו ומעמדו של העובד בארגון. חשבון גישה, שלא נעשה בו שימוש במשך תקופה העולה על 90 יום, יינעל לשימוש וייפתח רק באישור הממונה על הגנת המידע בכללית.

7.9.8. הוראות עבודה פרטניות יסדירו את תהליכי ניהול הרשאות ומשתמשים בכללית, לאורך מכלול שלבי הטיפול בהרשאות המשתמש, דרכי אימות הזהות, ניהול והקצאת הרשאות, בקרה שוטפת וסקירה תקופתית.

7.9.9. סיסמאות גישה יעמדו בקריטריונים שייקבעו, מעת לעת, על ידי הממונה על הגנת המידע בכללית בשיתוף אגף מחשוב ומערכות מידע. הסיסמאות יוגנו באמצעות הצפנה לכל מכלול מחזור השימוש בהן.

7.9.10. חשבונות גישה של משתמשי "מערכת" (Service Accounts) ייחסמו לגישה אינטראקטיבית.

7.9.11. כל התחברות לבסיס נתונים של הכללית חייבת להיעשות בזיהוי באמצעות חשבון משתמש ייעודי ובאישור מראש של הממונה על הגנת המידע בכללית בשיתוף אגף מחשוב ומערכות מידע.

7.9.12. לכל מערכת מידע ייקבע איפיון (פרופיל) של הרשאות עבור המשתמשים בהתאם לתפקידם. קביעת האיפיון באחריות רפרנט המערכת /הלקוח העסקי.

7.9.13. הקצאת הרשאת גישה למשתמש, החורגת מהאיפיון (מהפרופיל) שנקבע למערכת, מחייבת אישור פרטני בידי וועדת הרשאות חריגות בראשות הממונה על הגנת המידע בכללית.

7.9.14. פתרונות מחשוב, ישומים חדשים ושינוי גרסה משמעותיים המפותחים על ידי הכללית או בעבורה יתוכננו ויפותחו באופן שניתן יהיה לקיים מידרג של מנהלי מערכת (ADMIN). תתוכנן שכבת מנהל ראשי (super user) אשר יהיה בעל הרשאות מקסימליות ובעל יכולת לקבוע הרשאות למנהלי מערכת תחתיו. הזדהות והרשאות של משתמשים בעלי הרשאות עודפות (פריוילגיות), מנהלי מערכת ואנשי IT ותמיכה תהיה הזדהות חזקה וחד ערכית משאר משתמשי הארגון.

7.9.15. גישה ושימוש במידע ינוטרו ויבוקרו באופן פרטני בכדי להבטיח מתן דין וחשבון אישי.

7.9.16. בקרת הרשאות משתמש תבוצע בשלוש רמות:

א. רפרנט המערכת - בקרת הרשאות שנתית במטרה לאתר הרשאות ומשתמשים חריגים.

ב. מנהל מחשוב מוסדי – בקרת משתמשים שנתית במערכות המידע בהן הוא מעניק הרשאות.

ג. ממונה על הגנת המידע בכללית – בקרה על רפרנט המערכת ומנהל המחשוב המוסדי.

7.10. **<u>הגנה על הרשת וגישה מרחוק</u>**

7.10.1. ככלל, כל הקישורים לרשת הכללית וממנה, ינוהלו באופן מרוכז, על בסיס נקודות גישה מבוקרות ומנוהלות. ביצוע קישור לרשת הכללית מחייב אישור הממונה על הגנת המידע בכללית טרם הפעלת הקישור.

7.10.2. מנהלי רשת, מנהלי מערכות, טכנאים, מפתחים וכיו"ב גורמי פיתוח תפעול ותחזוקת מערכות מידע אינם רשאים, גם לא באופן זמני, להפסיק או לשנות את אופן פעולתו של מנגנון אבטחת מידע, או לחרוג מהוראות הגנת המידע בכללית, אלא אם התקבל לכך אישור מראש של הממונה על הגנת המידע בכללית. במקרים של צורך תפעולי דחוף בו לא ניתן לאתר את הממונה על הגנת המידע בכללית, יספיק אישור של ראש אגף מיחשוב ומערכות מידע. במקרה כזה יש ליידע את הממונה על הגנת המידע בכללית בהקדם.

7.10.3. גישה מחוץ לארגון למערכות הארגון מותנה בהזדהות חזקה חד ערכית, כהגדרתה בנוהל זה, של המשתמש והתחנה ממנה הוא מתקשר.

7.10.4. גישה מרחוק למערכות המידע של הכללית דורשת אישור מראש ממספר גורמים:

א. מנהל מוסד/ מחוז/ בית חולים/ ראש חטיבה/ חברת בת.

ב. ראש אגף מחשוב ומערכות מידע או מי מטעמו.

ג. הממונה על הגנת המידע בכללית.

7.10.5. כל סוג גישה מרחוק, שמחוץ לארגון, למערכות המידע בארגון או בבעלות הארגון, לרבות גישה באמצעות תווך סלולרי, ייעשו על פי סטנדרטים שיקבעו על ידי הממונה על הגנת המידע בשיתוף אגף המחשוב ומערכות מידע ובכפוף לנאמר בסעיף 3.6.3 לעיל.

7.10.6. כל שימוש ברשתות או בתווך אלחוטי, מכל סוג שהוא, מותנה באישור מראש של הממונה על הגנת המידע בכללית, אשר יקבע את אופן השימוש ותנאיו, בכפוף לעמידה בדרישות הגנת המידע.

7.10.7. מערכות תומכות חיים, לרבות מעבדות, פגיות, מערכות טיפול נמרץ וציוד מנתח, יחוברו ויפעלו ברשת תקשורת נפרדת ומוגנים באמצעות מנגנוני בידוד על פי הנחיות הממונה על הגנת המידע בכללית. כך גם מערכות על פי הנחיית משרד הבריאות והרשות לאבטחת מידע בשב"כ (שהוגדרו כתשתית קריטית).

7.11. **<u>דואר אלקטרוני, מערכות העברת מסרים, אינטרנט</u>**

7.11.1. האינטרנט מהווה סכנה לשלמות, זמינות וסודיות המידע הארגוני. לא יועבר מידע "חסוי" או "חסוי אישי" על גבי תשתיות רשת האינטרנט למעט הצגת נתוני אדם לפי הרשאת אותו אדם בלבד. אלו יוצגו באתר כללית On Line, או בהסכמה מיוחדת של אותו אדם לגביו מתייחס המידע על גבי טופס, לפי נוהל מסירת מידע רגיש 08-01-02.

7.11.2. תחסם גישה לשירותי האינטרנט המהווים סכנה לשלמות, זמינות וסודיות המידע.

7.11.3. מידע "חסוי אישי" יכול להשלח לנמעני רשת הדואר הארגוני בתנאי שכתובת המייל מסתיימת ב- @clalit.org.il.

7.11.4. הודעת דואר אלקטרוני, <u>אל מחוץ לכללית</u>, שיש בה מידע "חסוי אישי" יכולה להשלח ללקוח/למטופל או לעובד או לבא כוחו כחוק, רק אם אישר והסכים לכך הלקוח/ מטופל/ עובד מראש ובכתב או באישור הממונה על הגנת המידע בכללית.

7.11.5. הודעת דואר אלקטרוני "חסוי אישי" תאובטח באופן שלא ניתן יהיה לקרוא את תוכנה אלא על ידי הנמען לו נועדה ההודעה ובכפוף לסעיף 5.14.

7.11.6. עובד אינו רשאי להפעיל בתיבת הדואר שלו בכללית הגדרה של העברה/הפנייה אוטומטית של מסר אלקטרוני שהגיע אליו לכתובת דואר אלקטרוני אל מחוץ לכללית.

7.11.7. במערכת הדואר האלקטרוני המרכזית והמוסדית תחסם האפשרות לבצע הפנייה אוטומטית של דואר אלקטרוני מתוך הארגון לכתובת מחוץ לארגון.

7.11.8. מערכת העברת מסרים אלקטרונית (מסנג'ר) יכולות לפעול רק בתוך הרשת הארגונית ללא אפשרות להתחבר לגורם מחוץ לרשת הכללית ו/או האינטרנט.

7.11.9. כל הדיווחים שהכללית אמורה לדווח/להעביר למוסדות השלטון במדינה או חברות בנות יבוצעו באמצעות מערכת כספות וירטואלית, אשר תצפין את המידע ותאפשר גישה על בסיס זיהוי חד ערכי של הגורם אליו נשלח המידע.

7.11.10. כל אתר אינטרנט של הכללית וחברות בנות, כולל שינויי גרסה באתר, יעברו בדיקות חוסן למניעת פגיעה בשלמות, זמינות וסודיות המידע טרם "עלייתם לאוויר" ולפחות פעם בשנה.

7.12. **<u>הלבנת תוכנות/חומרה/מידע</u>**

7.12.1. במצב בו נדרש לשלב למערכות הארגון תוכנה/חומרה/מידע שלא נרכש/פותח/נוצר בכללית, יש להעביר מראש את החומרה/תוכנה/מידע ליחידת המחשוב במוסד/ מחוז/ ההנהלה הראשית לשם בדיקת הגנת מידע והתאמה לסטנדרט הגנת המידע בכללית, טרם שילובם במערכות הכללית. כך גם לגבי הורדת קבצים מהאינטרנט ושילובם במערכות הכללית.

7.13. **<u>ניטור ותגובה לאירועים</u>**

7.13.1. באחריות הממונה על הגנת המידע בכללית לוודא כי מבוצע ניטור של מערכות המידע לצורך זיהוי חריגות אבטחה. פעולת הניטור הינה באחריות צוות אבטחת מידע באגף מחשוב ומערכות מידע.

7.13.2. מערכות מידע, לרבות מערכות רפואיות יתוכננו תוך שילוב אפשרות לקבלת מידע מלא על כל הפעילות המתרחשת במערכת בפרוט של:

א. מי המשתמש שפנה למערכת.

ב. מאיזה תחנה פנה למערכת.

ג. תאריך ושעה שפנה למערכת

ד. מה הפעולה שביצע במערכת.

7.13.3. הדרישה לקבלת מידע על הפעילות המתרחשת במערכת נועדה על מנת לזהות פעילות בלתי מורשית או תחקור של אירועים. כמו כן, תתוכנן ותשולב במערכות אלו, אפשרות לקבלת התרעות הגנת מידע, זיהוי כשלים, תהליכי תגובה מיטביים וזיהוי אנומליות. במערכות הקיימות ישולב נושא זה באופן הדרגתי.

7.13.4. יוגדרו נוהלי תגובה לארוע, לרבות דרכי דיווח, פעילויות תגובה והתנאים בהם יופעלו.

7.13.5. כל ארוע של פגיעה בהגנת המידע יתוחקר כדי לאתר את סיבת השורש להתרחשות האירוע ולוודא מניעת הישנות מקרים בעתיד. דו"ח הארוע והתחקיר יועבר ליו"ר וועדת אתיקה עליונה להגנת מידע, לידיעת סמנכ"ל וראש חטיבת לוגיסטיקה תשתיות ומערכות מידע והממונה על הגנת המידע בכללית.

7.14. **<u>הגנה על תחנות קצה / שרתים (ובכפוף לסעיף 5.14)</u>**

7.14.1. לא יישמר כל מידע על תחנת קצה תפעולית של משתמש. בפרט, לא יישמרו תכתובות דואר, קבצי נתונים, גיליונות אלקטרוניים וקבצי גיבוי.

7.14.2. תחנות קצה /שרתים בכללית יותקנו ויוקשחו בהתאם להנחיות הגנת המידע הרלבנטיות. בפרט, יוקשחו שרתים שיש להם קישור לאינטרנט.

7.14.3. תחנות הקצה /שרתים בכללית ייסרקו באופן תקופתי, אחת לרבעון, לזיהוי חולשות אבטחה שעלולות לפגוע ברמת ההגנה.

7.14.4. בכדי להגן על המידע מנוזקות, ישולבו בכל מערכות המחשב אמצעי זיהוי ומניעה מתאימים, לרבות אנטי-וירוס.

7.14.5. ככלל, חל איסור על שימוש בהתקנים חיצוניים וקישורם למערכות הכללית, פרט לאלו שאושר השימוש בהם. בכל מקרה של קישור התקן חיצוני למערכות הכללית, יעבור ההתקן סריקה של אנטי-וירוס טרם חיבורו, כברירת מחדל.

7.14.6. בכדי לשמור על רמת הגנת המידע, יעודכנו המערכות הרלבנטיות בקובצי החתימות ובטלאי האבטחה הקריטיים , בהתאם להנחיות הממונה על הגנת המידע בכללית

7.14.7. תחנות קצה שאינן מקושרות לרשת תקשורת (Stand Alone) יעודכנו בטלאי אבטחה וחתימות אנטי-וירוס באחריות מנהל המחשוב של היחידה בה מוצבת התחנה. תדירות העדכונים השונים תקבע בהתאם לנסיבות ולהנחיות הממונה על הגנת המידע בכללית.

7.15. **<u>מחשוב נייד (ובכפוף לסעיף 5.14)</u>**

7.15.1. לא יחובר למערכות המידע ו/או המערכות הרפואיות של הכללית מכשיר קצה נייד מכל סוג שהוא (לרבות סמארטפון), אלא על פי סטנדרטים שיקבעו על ידי הממונה על הגנת המידע בשיתוף אגף מחשוב ומערכות מידע.

7.15.2. בפרט לא יחובר מכשיר קצה כאמור אלא אם הופעל בו מנגנון אבטחה המייצר בידוד בין סביבת ההתחברות לכללית לסביבת העבודה הרגילה של המכשיר.

7.15.3. חל איסור מוחלט על שימוש במצלמות של התקני הקצה במתקני הכללית. בפרט, אין לצלם תמונות שמהן ניתן לזהות פני אדם (איש צוות או מטופל) או פרטי מידע חסוי. במידה ועולה צורך לצלם תמונות כאמור, יש צורך לקבל את אישורו של אותו אדם מראש ובכתב.

7.15.4. מותר לצלם פעולות רפואיות שאין בהן פרטים מזהים של אדם פלוני.

7.16. **<u>המשכיות עסקית</u>**

7.16.1. על מנת למנוע פגיעה ברציפות התפקודית של הכללית תגובש תוכנית המשכיות עסקית כוללת. האחריות לכך חלה על מנהל שבתחום אחריותו פועל /קיים נכס מידע.

7.16.2. תוכנית ההמשכיות העסקית תכלול התייחסות מיוחדת לאיומי סייבר (Cyber).

7.16.3. יתבצע תרגול תקופתי לבדיקת תוכנית ההמשכיות ויכולת ההתאוששות מאסון, לרבות שחזור מידע מגיבוי, בתדירות שתקבע ובהתאם להנחיות הממונה על הגנת המידע בכללית.

7.16.4. בכל מוסד תייחד ההנהלה, אחת לשנה, דיון בנושא המשכיות עסקית.

7.16.5. תשתיות המידע והתקשורת ייבנו באופן שיאפשר את השרידות התפקודית הנדרשת, גם כאשר אלו מצויים תחת התקפה.

7.16.6. במערכות המידע ישולבו פתרונות שרידות, גיבוי והתאוששות בהתאם לסיווג המידע ו/או על פי החלטת וועדת אתיקה עליונה להגנת מידע.

8. תהליכי פיתוח, רכש ותחזוקת מערכות

8.1. **כללי**

8.1.1. החלת מדיניות הגנת המידע, דורשת התייחסות קפדנית למספר ממדים בארגון ממדים אלה הנם:

א. אבטחה פיזית על המידע

ב. הגנת מידע במערכות המידע

ג. הגנת מידע במערכות משובצות מחשב/מכשור וציוד רפואי

ד. הגנת מידע בתקשורת קווית ואלחוטית

ה. הגנת מידע בתהליכי בינוי ותשתיות

ו. המימד האנושי

ז. בקרה על הגנת המידע

ח. שרידות מידע ומערכות גיבוי

ט. הגנת מידע בתרבות הארגונית

י. השמדת המידע

8.1.2. בכל תהליך, בין אם הוא חדש ו/או שינוי גרסה/ תצורה משמעותי, ו/או יצירת קישור לוגי בין שתי מערכות (למשל על ידי יצירת Web Services), בארגון או מחוץ לארגון, מתחייבת מעורבות הממונה על הגנת המידע בכללית, החל משלב אפיון התהליך, על מנת לוודא מתן רמה נאותה של הגנת המידע.

8.1.3. ככלל, רכש מערכות מידע ו/או מערכות רפואיות (להלן: "המערכת") מחייב עמידה בסטנדרט אבטחת המידע שיקבע הממונה על הגנת המידע בשיתוף אגף מחשוב ומערכות מידע.

8.1.4. כל ממשק של מערכת מידע או שירות עם מערכת מידע שיש בה מידע "חסוי אישי" מחייבת אישור הממונה על הגנת המידע בכללית.

8.1.5. בפרט, רכש והצטיידות <u>בכלים ומערכות לאבטחת מידע</u> ייעשה בהתאם לדרישות ההגנה של הממונה על הגנת המידע בכללית, ובאישורו כי הפתרון המוצע עונה על צרכי האבטחה. טרם הפעלת הכלים יש לקבל את אישור הממונה על הגנת המידע בכללית כי אופן הפריסה של המערכת והגדרות התצורה שלה עונות על דרישות הגנת המידע בכללית. ההחלטה בדבר סוג הציוד היא בידי אגף מחשוב ומערכות מידע.

8.1.6. האחריות על שילוב הגנת מידע בתהליך ויישומה חל על יוזם התהליך או על הרפרנט/בעל המידע. הרפרנט יוודא שגורמי הביצוע משלבים את הגנת המידע בהתאם.

8.1.7. כל תהליך כאמור, שכתוצאה ממנו עשוי להיות מופק או מעובד מידע, יסווג ברמת רגישות על ידי יוזם התהליך או ע"י הרפרנט (אם הוגדר) אלא אם וועדת אתיקה עליונה קבעה אחרת.

8.1.8. מידע אמיתי יימצא <u>רק בשרתי ייצור</u> (production) ובבסיסי נתונים המשרתים את הייצור. בשרתי פיתוח, שרתי בדיקות, שרתי הדרכה יעשה שימוש במידע לא אמיתי ובכפוף לסעיף 5.14 לעיל.

8.2. **<u>ייזום התהליך</u>**

8.2.1. ראש אגף מחשב ומערכות מידע יודיע לממונה הגנת המידע בכללית ,על כל ייזום שאושר. מסמכי הייזום הרלבנטיים יועברו להתייחסות הממונה על הגנת המידע בכללית, אשר יביע את דעתו בנושא הגנת המידע והמשמעויות הנגזרות מבחינת הגנת המידע בכללית.

8.2.2. ייזום מערכת מידע שאושר ובמערכת מתוכנן להימצא או לעבור מידע מסווג "חסוי-עסקי" או "חסוי אישי" על יוזם המערכת להקים וועדת אתיקה להרשאות.

8.2.3. תקציב הגנת מידע - תקציב הגנת מידע בתהליך/פרויקט/שינוי גרסה משמעותי/פרויקט רכש/פרויקט בינוי יהיה חלק מתחשיב עלות הפרויקט/תהליך. עלויות תגובה לאירועי הגנת מידע יועמסו על תקציב הפרויקט/תהליך. עלויות הגנת מידע אחרות יתוקצבו במסגרת דרישת תקציב שנתית של אגף מחשוב ומערכות מידע והנהלת המוסד.

8.3. **<u>איפיון והגדרת דרישות</u>**

8.3.1. סיווג המידע יכתיב את דרישות הגנת המידע בהתאם לדרישות החוסן (הוראות עבודה להגנת המידע ראה הוראה 800-02-02) ואישור הממונה על הגנת המידע בכללית. דרישות אלו ישולבו בפרק הגנת מידע במסמך האיפיון.

8.3.2. כתיבת פרק הגנת המידע במסמך האיפיון – באחריות הממונה על הגנת המידע בכללית בהתייעצות עם הגורם המפתח.

8.3.3. כפועל יוצא מדרישות הגנת המידע במסמך האיפיון מטעם הממונה על הגנת המידע בכללית, ייכתב בנספח הטכני של מסמך האיפיון, פרק אבטחת מידע – באחריות ראש אגף מחשוב ומערכות מידע/מנהל מחשוב במוסד.

8.4. **<u>פיתוח/רכש/חוזה התקשרות</u>**

8.4.1. ככלל, מערכות המידע המפותחות בכללית, או עבור הכללית, יפותחו בתהליך של "פיתוח מאובטח" בהתאם לדרישות ההגנה שהוגדרו בשיתוף הממונה על הגנת המידע בכללית.

8.4.2. עובד המועסק בפיתוח מערכת מידע יפתח את המערכת "פיתוח מאובטח" המותאם לשפת הפיתוח.

8.4.3. בכל חוזה התקשרות עם ספקים ויועצים, מכרז, תוכנית בינוי, יציאה ל- R.F.P בין אם מדובר התהליך חדש או שינוי גרסה, בהם עשוי להיחשף מידע "חסוי עסקי" או "חסוי אישי", או שיש בשירות צורך בגישה או חיבור לרשת התקשורת של הכללית, ישולבו פרק הגנת מידע, נספחי הגנת מידע ושמירה על סודיות, בהתאם להנחיות הממונה על הגנת המידע בכללית. הנוסח הסטנדרטי של הנספחים האמורים ייעודכן אחת לשלוש שנים.

8.4.4. אחריות שילוב פרק הגנת המידע חלה על מנהל הפרוייקט/רפרנט המערכת.

8.4.5. כל מנהל אליו כפופים מפתחי אפליקציה, או מתכנני תשתית יוודא כי אלו הוכשרו לנושאי הגנת מידע ושיטות לפיתוח מאובטח.

8.5. **<u>שלב הבדיקות/ניסוי/הערכה</u>**

8.5.1. ככלל, מידע אמיתי יימצא רק בשרתים ומערכות בייצור. המידע שמשמש בסביבות בדיקות/ניסוי/הערכה או פיתוח יהיה מידע לא אמיתי (מידע דמה).

8.5.2. בכל מערכת מידע ובפרט בציוד/מכשור רפואי אשר נמצאים בשלב של ניסוי/ בדיקה/ הערכה יש לוודא הסרה מלאה של הנתונים שנצברו במכשיר טרם בתום הבדיקה. יש לוודא יכולת הסרת מידע כאמור בטרם תחילת הבדיקה. "כללית הנדסה רפואית" ועובד הכללית האחראי על ביצוע הבדיקה אחראים לוודא קיום דרישה זו.

8.6. **<u>שלב הפעלה / ייצור</u>**

8.6.1. קיום הדרישות בפרק הגנת המידע כאמור, הינו תנאי לאישור/הפעלת התהליך, מכרז, חוזה התקשרות, אישור בניה.

8.6.2. בפרט, מערכת חדשה, מערכת לאחר שינוי גרסה משמעותי לא תאושר להפעלה/שימוש בסביבת הייצור אלא לאחר שעברה בדיקות חוסן.

8.7. **<u>תחזוקה שוטפת/ שדרוגים ועדכונים</u>**

8.7.1. אחת לשנה יבצע רפרנט המערכת סקירה ואשרור של משתמשים והרשאות במערכת. הרפרנט יתעד את ממצאי הסקירה ויאשר בחתימתו את מצב המשתמשים וההרשאות לאחר ביצוע השינויים הנדרשים, אם היו כאלה. הממונה על הגנת המידע בכללית יוודא ביצוע סקירה תקופתית כאמור.

8.8. **שלב גריעה**

8.8.1. כל ציוד מחשוב ו/או מכשור רפואי ו/או רכיב זכרון/או מדיה, המכילים מידע רגיש או חסוי, שמיועדים להפסקת פעילות/מכירה/השמדה, יעברו תהליך ניקוי והסרה של מידע, בהתאם להנחיות הממונה על הגנת המידע בכללית.

8.9. מידע, בין אם מסמכים או רכיבי זיכרון, יושמד רק בדרך של גריסת פתיתים באופן שלא ניתן לשחזר את המידע או לעשות שימוש ברכיבי הזיכרון.

8.10. הגנת המידע בתהליכים השונים תתבצע בשבעה שלבים:

מס	שלב	שלוב הגנת מידע	גורם האחראי על הביצוע
1	**ייזום שאושר לביצוע**	הבנת התהליך, סוג המידע, דרישות סף להגנת המידע וסיווג המידע	היוזם + בהתייעצות עם הממונה על הגנת המידע בכללית
2	**שלב הגדרת דרישות (שלב האפיון)**	קביעת דרישות הגנת מידע ע"פ דרישות החוסן בהתאם לסיווג המידע שנקבע לתהליך והוראות עבודה הממונה על הגנת המידע בכללית. הגדרת התקציב.	האחראי על התהליך בשיתוף ובאישור הממונה על הגנת המידע בכללית
3	**שלב יישום הדרישות**	שילוב מענה לדרישות בשלב הפיתוח ו/או הרכישה	גורם מפתח.
4	**שלב בדיקות**	בדיקת חוסן וישימות	גורם מפתח באמצעות הממונה על הגנת המידע בכללית, צוות בדיקות
5	**שלב הפעלה/ ייצור**	אישור היישום	וועדת היגוי להגנת מידע / הממונה על הגנת המידע בכללית
6	**שלב בקרה שוטפת**	בקרה על קיום נהלי הגנת המידע אישור הרשאת גישה של משתמש לתהליך	גורם מתפעל רפרנט המערכת.
7	**שלב גריעה**	השמדה מבוקרת של מידע ורכיבים אחרים	נאמן הגנת מידע/רפרנט המערכת