נוהל סיווג מידע **ISO 27799**	
מהדורה	2.0
בתוקף מ	ינואר 2018
א.8	עמוד 1 מתוך 25

ניהול אישורים

תאריך	שם	תפקיד	חתימה
30/09/2012	שי אמיר	ממונה אבטחת מידע	שי
01/03/2016	שי אמיר	ממונה אבטחת מידע	שי
01/08/18	ראובן אליהו	ממונה אבטחת מידע	ראובן

ניהול שינויים

תאריך	מחבר	גרסא	מהות השינוי
1/3/07	רן אדלר	1.0	מסמך ראשוני
1/5/07	יהושע פסין	1.1	עריכה
8/8/07	יהושע פסין	1.2	שינוי בסעיף 5.2.3 - הוספת סטנדרט למגרסות
9/8/09	מורנו נאור	1.3	מספור הנוהל בהתאם לתקן.
09/02/2012	טליה זמיר יהושע פסין	1.4	התאמה לתקן ISO 27799
22/08/2012	טליה זמיר תמיר פלדמן	1.5	התאמה לתקן ISO 27799
17/11/2014	אורנסק	1.7	התאמות לדרישות תקן ISO 27001:2013 עדכון סעיף 5.1.3 ביטול סעיפים 5.3.1 ו- 5.3.2

נוהל סיווג מידע **ISO 27799**	
מהדורה	2.0
בתוקף מ	ינואר 2018
א.8	עמוד 2 מתוך 25

21/07/2015	גבי פטליס	1.8	בקרה
06/03/2018	גבריאל כהן	1.9	עדכון איסור גישה לאינטרנט משרתי אפליקציה ושרתי בסיסי נתונים מרשתות המוגדרות כחסוי
01/01/2018	אורנסק	2.0	התאמה לתקן ISO 2016:27799

1. <u>מטרה</u>

1.1. קביעת כללים לסיווג מידע במשרד הבריאות

1.2. קביעת כללים להעברת מידע על פי רמת הסיווג של המידע – נספח א'

2. <u>הגדרות</u>

2.1. משתמש - עובד הארגון או גורם חיצוני, אשר במסגרת תפקידו משתמש במערכות מידע.

2.2. מאגר מידע – מקבץ נתונים המאוחסן באמצעי ממוחשב.

2.3. מידע פומבי – מידע אשר אין למשרד הבריאות צורך להגן על סודיותו, והגישה אליו מותרת לכל אדם, באשר הוא, לכל מטרה. לדוגמא: נתונים אשר מפורסמים בעיתונות.

2.4. מידע חסוי / חסוי ביותר– מידע אשר חשיפתו לגורם בלתי מוסמך עלולה לגרום למשרד הבריאות נזק או שעצם חשיפתו מהווה עבירה על החוק.

2.5. נכס מידע – מערכת מידע או מצע פיזי האוגרים מידע בעל ערך למשרד הבריאות או מאגר מידע כמוגדר בחוק הגנת הפרטיות. ההתייחסות בנוהל זה היא רק לנכסי המידע הנמצאים בבעלות משרד הבריאות ומבוקרים על ידו. (לחדד: נכס יכול להיות תהליך עבודה קבוע שגוזר בסופו של תהליך עבודה).

2.6. בעל נכס מידע - האחראי על המידע, על שינויו ו\או ההשפעה אשר תהיה לאובדנו על הפעילות הארגונית.

2.7. מצאי – מונח לוגיסטי המקביל למונח נכס.

2.8. מלאי - ציוד זמין בבעלות העסק המשמש לצורך פעילותו העסקית השוטפת.

3. <u>מסמכים ישימים</u>

3.1. נהלי מסגרת לאבטחת מידע - משרד ראש הממשלה 2005

3.2. נוהל אבטחת מידע – **א 18.1 התאמה לדרישות שע"פ דין**

4. <u>אחריות ליישום הנוהל</u>

4.1. כלל המנהלים והעובדים (כולל עובדים חיצוניים) במשרד הבריאות.

4.2. מנכ"לים בארגוני הבריאות ומטעמם אנשי המחשוב המבצעים.

4.3. מנהלי בתי חולים.

4.4. מנמ"ר ו/או מנהל אבטחת מידע של כל יחידה בבית חולים ומרכז רפואי.

4.5. מנמ"ר ו/או מנהל אבטחת מידע של כל קופת חולים.

4.6. כלל העובדים העוסקים בתהליך הפקת המידע או קליטתו.

4.7. אגף המחשוב – עובדים המעורבים בפרויקט לרבות מנהל הפרויקט וצוות הפיתוח.

4.8. מנהל אבטחת מידע משרד הבריאות.

5. <u>שיטה</u>

5.1. <u>תהליך סיווג המידע</u>

5.1.1. קביעת עקרונות לרמות סיווג של המידע תיעשה על-פי רגישותו. רגישות המידע תקבע על-פי מספר פרמטרים:

5.1.2. חיסיון הפרט - האם המידע מוגן מתוקף חוק הגנת הפרטיות.

5.1.3. חיסיון מסחרי – האם חשיפת המידע תגרום לנזק פיננסי פנימי או חיצוני.

5.1.4. היקף הנזק שעשוי להיגרם עקב חשיפת המידע.

5.2 <u>רמות הסיווג הקיימות הינן:</u>

5.2.1 **בלמ"ס** – מידע גלוי.

5.2.2 **חסוי** – מידע עסקי, מידע רפואי, מידע על עובדים.

5.2.3 **חסוי ביותר** – כמפורט בנספח א' סיווג מידע במערכת הבריאות במסמך זה.

5.2.4 רמת סיווג למסמכים, אשר קשה לסווגם ע"פ העקרונות הכלליים שנקבעו, תקבע ע"י מנהל אבטחת המידע ומנהל מאגר המידע הרלוונטי בהתייעצות עם היועצת המשפטית של משרד הבריאות.

5.2.5 כל סוג מידע חדש הנכנס לשימוש במערכת הבריאות יסווג ע"פ הקריטריונים שנקבעו. במקרה של ספק, יקבע הסיווג ע"י מנהל/בעל המאגר.

5.2.6 קביעת רמת רגישות נכס המידע נקבעת ע"פ רמת רגישות המידע הגבוהה ביותר אשר כלול בנכס המידע. כך, במידה ובנכס מידע קיים פריט מידע רגיש או אוסף פריטי מידע אשר יוצרים אפיון של מידע רגיש, כל הנכס יוגדר כרגיש.

5.3 <u>פרמטרים לקביעת סיווג המידע :</u>

5.3.1 טרם קביעת סיווגו של פריט מידע, מצע מידע או מערכת מידע, יש לשקול את מידת השפעתם או מידת הרלוונטיות של הפרמטרים הבאים.

5.3.2 ככל שמידת ההשפעה או הרלוונטיות של אותו פרמטר היא גבוהה יותר, כך ניתן להסיק כי המידע רגיש יותר ויש לסווגו ברמת סיווג גבוהה יותר.

5.3.3 להלן פרמטרים לקביעת סיווג המידע -

5.3.4 מידת הנזק - מידת הנזק שיגרם למשרד הבריאות / ללקוחותיה / לעובדיה, במידה והמידע יפגע ו/או יגיע ל"ידיים בלתי רצויות".

5.3.5 ערך המידע - ערכו של המידע בעיני גורמים בעלי "אינטרסים שליליים" (גורמים עבריינים/ יריבים עסקיים וכד'), במידה ויגיע המידע לידיהם.

5.3.6 מחויבות חוקית - פגיעה פוטנציאלית במשרד הבריאות ו/או בעובדי משרד הבריאות משום הפרת מחויבות חוקית. אפשרות זו נובעת לרוב מסיווג מידע לקוי והמשך טיפול בלתי הולם במידע, נסיבות המגדילות את אפשרות הפגיעה במידע ו/או הגעתו של מידע לידי "ידיים בלתי רצויות".

5.3.7 עיתוי - רמת הרגישות עשויה להשתנות על ציר הזמן. מצע מידע יישא רמת רגישות גבוהה ביותר עד לרגע פרסומו והפיכתו לנחלת הכלל (לדוגמה, מחקר יהיה רגיש ביותר עד פרסומו ולכן סיווגו של המידע יהיה רגיש ביותר עד לשלב זה).

5.3.8 רמת פירוט - ככל שרמת פירוט הנתונים גבוהה יותר, כן תהיה רמת רגישות המידע גבוהה יותר ומידת הנזק גדולה יותר, היה והמידע יגיע ל"ידיים בלתי רצויות".

5.3.9 כמות - ככל שכמות המידע המצוי במצע המידע גדולה יותר, כך הנו רגיש יותר ומידת הנזק תהיה גדולה יותר, במידה והמידע יגיע ל"ידיים בלתי רצויות".

5.4 <u>שיטת עבודה לקביעת סיווג נכסי מידע:</u>

5.4.1 איסוף מידע -

5.3.1.1 בשלב זה מבוצעים ראיונות עם בעלי תפקידים רלוונטיים (בעלי המידע), במטרה ללמוד על נכסי המידע שהם בעליו, על תהליכי העבודה, רגישות המידע, היקפי ותצורת חשיפתו או הפצתו, הסביבות הטכנולוגיות השונות בו ימצא המידע, חתכי המשתמשים העושים שימוש במידע וצרכי הנגישות אליו.

5.3.2 הגדרת רמות סיווג וקריטיות לנכסי המידע -

5.3.2.1 הגדרת רמות הסיווג והקריטיות של נכסי המידע מתבצעת בשיתוף עם בעלי המידע ובעלי התפקידים. פעילות זו נגזרת מהמידע שנאסף בשלב הקודם. לבעלי התפקיד הוצגו רמות הסיווג והקריטיות הקיימות ועליהם היה לאשר כי הן מתאימות לסוגי נכסי המידע שבאחריותם.

5.3.2.2 בנוסף לסיווג המידע ע"ב רגישותו לגילוי יש לסווג את קריטיות המידע, מידת הזמינות והשלמות של המידע.

5.3.2.3 יש לשים דגש על תהליכים קליניים הדורשים זמן התאוששות מסוים בעת קביעת דרישות הזמינות למידע בריאותי אישי.

5.3.2.4 סיווג המידע ביחס לזמינות, שלמות וקריטיות צריך להיות מיושם גם על תהליכים, התקני IT, תוכנה, מיקומם וכוח אדם.

5.3.2.5 יש לזהות את הקריטיות של נכסי המידע והתהליכים לפעילות העסקית של הארגון על ידי ניהול סיכונים.

5.3.3 סיווג מערכות מידע חדשות -

5.3.3.1 בעת תכנון מערכת חדשה או שינוי במערכת קיימת יש לבצע סיווג מידע על בסיס הערכת סיכונים שתבוצע למערכת.

5.3.3.2 הערכת הסיכונים תבוצע לפי הוראות נוהל זה.

5.4 <u>שיטה לסיווג מערכות מידע</u>

5.4.1 כלל האפליקציות בארגון ימופו לתוך טבלה.

5.4.2 הטבלה תכיל נתונים טכניים הנוגעים במערכת כגון:

5.4.2.1 למה משמשת המערכת

5.4.2.2 איזה סוג מידע מכילה

5.4.2.3 כמה משתמשים במערכת

5.4.2.4 האם המערכת היא בעלת ממשקים למערכות אחרות או לאינטרנט

5.4.2.5 בעל המידע (תפקיד)

5.4.2.6 האם נתמכת ע"י ספק חיצוני ע"י חיבור מרחוק?

5.4.2.7 האם נתונים מסווגים מוצפנים?

5.4.3 טבלה זו תשמש את המשרד לצרכים הבאים:

5.4.3.1 קביעת רמת הסיכון והקריטיות של המערכות וגזירה, כתוצאה מכך, של רמת האבטחה אשר יש ליישם במערכות אלו וכן תדירות הבדיקות (סקרי סיכונים ומבחני חדירה) במערכות אלו.

5.4.3.2 תכנון נכון של מערך ה DRP שייקבע לפי רמת הזמינות הנדרשת מהמערכת.

5.4.4 רשימת שאלות בנושאים השונים:

5.4.4.1 סודיות

מס'	השאלה	מטרת השאלה	הציון
.1	האם המערכת חשופה לאינטרנט?	מערכות החשופות לאינטרנט נמצאות ברמת סיכון גבוהה יותר לדליפה של נתונים- על כן יש להגדיר כי הן נמצאות ברמת סיכון גבוהה יותר	-1 המערכת אינה חשופה לאינטרנט -3 המערכת מאפשרת חיבור מרחוק (כגון על ידי קונקטרה) של מספר גורמים מצומצם. -5 פתוח לאינטרנט באופן מלא
.2	האם המערכת אוגרת מידע	מערכות האוגרות מידע רפואי פרטני של אזרחים	-1 לא -3 כן- אוגרת מידע של פחות מ 1000

	רפואי של אזרחים?	הינן מערכות ברמת סיכון גבוהה על פי חוק הגנת הפרטיות.	אזרחים. 5- כן- אוגרת מידע של מעל 1000 אזרחים.
.3	האם הגישה למערכת מתבצעת באמצעות כרטיס חכם?	גישה באמצעות כרטיס חכם מקשה באופן ניכר על גורמים לא מורשים לחדור אל המערכת.	1- כן 3- 5- לא
.4	סביבת ההתקנה של המערכת	האם המערכת מותקנת ב: 1. סביבה מאובטחת ומבודדת 2. סביבה מאובטחת 3. סביבה לא מאובטחת	1. סביבה מאובטחת ומבודדת 3. סביבה מאובטחת 5. סביבה לא מאובטחת
.5	האם בוצע סקר סיכונים בעבר במערכת והאם הוטמעו הממצאים	מערכת אשר עברה בעבר סקר סיכונים וממצאיו יושמו- או בוצע בה תהליך של ליווי פיתוח מאובטח- רמת הסיכון לדליפת מידע בה- הולך וקטן.	1- בוצע תהליך פיתוח מאובטח+ סקר סיכונים שממצאיו יושמו. 2- בוצע תהליך פיתוח מאובטח בלבד 3- בוצע סקר סיכונים בלבד שממצאיו יושמו. 4- בוצע סקר ללא יישום ממצאים. 5- לא בוצע כלום.
.6	מיקור חוץ במערכת	במידה והמערכת מתוחזקת באופן שוטף על ידי גורם חיצוני- עולה רמת הסיכון של המערכת	1 – המערכת אינה מתוחזקת על ידי גורם חיצוני 3- המערכת מתוחזקת על ידי גורם

		לזליגת מידע	חיצוני. קיימת בקרה על גישת הגורם (כגון אישור מראש לכניסה למערכת, פתיחה של חוקים ב FW לפי קריאה וכו') ויש לספק זיהוי חזק כגון TOKEN 4- המערכת מתוחזקת על ידי גורם חיצוני. קיימת בקרה על גישת הגורם (כגון אישור מראש לכניסה למערכת, פתיחה של חוקים ב FW לפי קריאה וכו'). 5- יש גישה חופשית של גורם חיצוני אל המערכת.

5.4.4.2 זמינות

מס'	השאלה	מטרת השאלה	הציון
.1	האם חוסר זמינות המערכת מונע מהמשרד מידע הדרוש להתנהלות היומיומית אשר אינו יכול להיות מושלם באופן ידני?	ככל שההתנהלות היומית תלויה במערכת וקיים פחות ניירת עם המידע כך עולה חשיבות זמינות המערכת.	1- יש אפשרות לספק את המידע באופן מלא באופן ידני. 2- המידע קיים גם בניירת\ תיקים וניתן לאתר אותו באופן חלקי. 4- המידע קיים גם בניירת\ תיקים- אך אין אפשרות לאתר אותו באופן זמין. 5- יש מידע הקיים רק במערכת.
.2	תוך כמה זמן מעת נפילת המערכת יש להעלותה חזרה?	בהתאם לקריטיות של המערכת לארגון זמן ההעלאה לאויר לאחר קריסה מתקצר.	1- מעל 5 ימי עבודה 2- עד 5 ימי עבודה 4- עד 24 שעות 5- מיידית

.3	האם המידע במערכת צריך להיות זמין באופן מיידי לעיון חולים\ רופאים וכד' ?	רמת הקריטיות של המערכת עולה או יורדת בהתאם לחיוניות זמינות המידע הרפואי שבה בזמן אמת.	1- לא 5- כן
.4	האם בעת נפילת המערכת קיים חשש לחיי אדם?	מערכת מוגדרת קריטית כאשר קיים חשש לחיי אדם.	1- לא 5- כן
.5	כמה משתמשים יש במערכת?	ככל שיש יותר משתמשים במערכת, המערכת קריטית יותר להתנהלות המשרד.	1- עד 20 ועד בכלל 2- בין 21 - 200 4- בין 201 - 1000 5- מעל אלף
.6	האם המערכת/ מאגר רשום בפנקס המאגרים במשרד במשפטים?	התאמה לחוק הגנת הפרטיות דורשת לרשום מאגרים חסויים בפנקס המאגרים ולהן על המאגר בצורה נאותה.	1. כן 5. לא

5.4.4.3 אמינות

מס'	השאלה	מטרת השאלה	הציון
.1	האם מערכות אחרות מסתמכות על המידע המוחזק במערכת?	ככל שיותר מערכות מסתמכות על הנתונים במערכת, כך חשיבות דיוק הנתונים במערכת עולה.	1- לא, אף מערכת 3- כן, מספר מערכות 5- כן, הרבה מערכות
.2	האם שינויים במידע שמחזיקה המערכת עלולים לגרום לנזק למערכת הבריאות	מערכת מוגדרת קריטית כאשר היא מחזיקה מידע חיוני להתנהלות משרד הבריאות.	1- לא 5- כן

.3	האם שינוי בנתוני המערכת עלול להשפיע על חיי אדם?	מערכת מוגדרת קריטית כאשר קיים חשש לחיי אדם.	1- לא 5- כן
.4	האם בעת נפילת המערכת קיים חשש לחיי אדם?	מערכת מוגדרת קריטית כאשר קיים חשש לחיי אדם.	1- לא 5- כן
.5	כמה משתמשים יש במערכת?	ככל שיש יותר משתמשים קיים סיכון גדול יותר של פגיעה בשלמות הנתונים במערכת.	1- עד 20 ועד בכלל 2- בין 21 - 200 4- בין 201 - 1000 5- מעל אלף

5.4.4.4 מילוי ערכי התשובות לשאלונים במחשבון הערכת סיכונים יסייע בקביעת ערך לרמת הסיכון של המערכת.

5.4.4.4.1 על בסיס ניקוד השאלות, יחושב ערך ממוצע לכל היבט - זמינות, שלמות, חיסיון.

5.4.4.4.2 בכל מערכת תבוצע גם הערכת חשיבות של כל אחד מהיבטים אלה - משקולות.

5.4.4.4.3 אח״כ יבוצע ממוצע משוקלל המגדיר את רמת הסיכון במערכת.

5.4.4.4.4 השאלונים ימולאו באופן תקופתי, בכל פעם שתבוצע הערכת סיכונים.

5.4.4.4.5 הציון הסופי ישמש אמצעי להערכת רמת הסיכון ולהשוואת רמת הסיכון בין המערכות השונות:

5.4.4.4.6 להלן מחשבון הערכת סיכונים במערכת לדוגמא:

מחשבון הערכת סיכונים במערכת - דוגמא

שם המערכת					
תאריך ביצוע הערכה					
סרגל ערכים	1	2	3	4	5
	נמוך מאד	נמוך	בינוני	גבוה	גבוה מאד

הערכת משקולות

יש להעריך את המשקל של כל אחד מהיבטי אבטחת המידע במערכת (חיסיון, שלמות, זמינות) בערכים מ-1 (נמוך ביותר) עד 5. על הערכים לבטא את החשיבות של כל היבט במערכת בפני עצמו וביחס לאחרים.

משקל זמינות במערכת	משקל חיסיון במערכת	משקל אמינות במערכת
3	4	5

הציון

ציוני שאלות זמינות	ממוצע זמינות	ציוני שאלות חיסיון	ממוצע חיסיון	ציוני שאלות אמינות	ממוצע אמינות
1	1.8	5	4.6	4	3.2
2		5		3	
3		3		2	
2		5		3	
1		5		4	

ציון סופי	3.316666667

הסופי הינו ממוצע משוקלל של שלושת ההיבטים חיסיון, זמינות ואמינות, אשר נוקדו באמצעות השאלונים.

6 **<u>חתימה</u>**

נוהל סיווג מידע **ISO 27799**		
	מהדורה	2.0
	בתוקף מ	ינואר 2018
	א.8	עמוד 13 מתוך 25

מנהל אבטחת המידע הינו הבעלים של מסמך זה והינו האחראי לודא כי הנוהל תואם את הדרישות המובאות במנא"מ.

נספח א'

סיווג מידע במערכת הבריאות

והוראות לטיפול ושימוש במידע לפי סיווגו

טבלה זו מרכזת באופן תמציתי את ההוראות בנושא, ואינה מחליפה את הוראות החוקים והתקנות או הוראות שבנהלים המפורטים בעניינים אלה

סד'	פעולה	בלמ"ס	חסוי	חסוי ביותר
1.	**הגדרת סוג הנתונים בכל סיווג**	• מידע לא פרטני • מידע אגרגטיבי (שאין בו כדי לזהות אדם מסויים). • סטטיסטיקה • חוזרים • פרסומים • מידע כללי המופיע באינטרנט	• מידע פרטני מזוהה רפואי. • כל מידע פרטני מזוהה (גם שאינו רפואי או עסקי) שאינו בלמ"ס ואינו חסוי ביותר (כגון מידע על עובדים, פניות ציבור וכדומה)	מערכות **ייעודיות*** למידע פרטני ומזוהה בנושאים הבאים: • איידס • פסיכיאטריה • התמכרויות וסמים • הפסקות הריון • בדיקות גנטיות ונתונים גנטיים • בדיקות קשרי משפחה • תרומות זרע • תרומת ביציות • טיפולי פוריות • אימוץ • מקרי אונס או תקיפה מינית • מחלות מין • אלימות במשפחה כולל כל מידע פרטני מזוהה בנושאים אלה, לרבות זימון תורים. *מערכת ייעודית היא מערכת **שליבת פעילותה או מרבית המידע השמור בה** הוא בנושא מסוים; מידע בנושאים אלה עשוי להימצא במערכות שסיווגן חסוי ואין בכך להשפיע על סיווג המערכת

				כולה.
.2	**ניטור מערכות המחשוב**	ללא הנחיות מיוחדות	עפ"י חוזר מנכ"ל (18/12) בנושא הגנה על מערכות ממוחשבות, בדגש על סעיף 9.15 • בנושאים אלה - ניטור עפ"י ההוראות לסיווג חסוי ביותר: ○ מידע רפואי אישי של אח"מים. ○ מידע על רישיונות קנאביס רפואי. ○ תורמי ומושתלי אברים.	הפעלת חוקים ומנגנונים להתרעות במקרה של חריגות
.3	**הגנה פיזית**	ללא הנחיות מיוחדות	• מתחם מוגן • חדר נעול בעת שאינו מאוייש • שמירת מידע (נייר, מדיה) בארון או מגירה נעולים	• מתחם מוגן • שמירה בכספת • אם אין כספת אלא רק ארון/מגירה נעולים: יש לוודא כי המקום מצולם ע"י מצלמה במעגל סגור ומוגן באמצעות אזעקה
.4	**השמדה**	מיחזור או גריסה	• איסוף מרוכז של נייר לגריסה • גריסה מאובטחת בלבד ע"י ספק מורשה (חל איסור לשלוח חומר חסוי למיחזור) או: • גריסה מקומית באמצעות מגרסת פתיתים	• שמירת נייר בפח גריסה נעול (או פח בחדר נעול) עד לגריסה. • גריסה מאובטחת בלבד ע"י ספק מורשה (חל איסור לשלוח חומר חסוי ביותר למיחזור) או: • גריסה מקומית, מיד בתום השימוש,

			• סוגי מדיה שאינם נייר יש להשמיד באמצעים מתאימים. באופן שלא יאפשר איחזור המידע • אין להשתמש בנייר עודף כניירות טיוטה	באמצעות מגרסת פתיתים • סוגי מדיה שאינם נייר יש להשמיד באמצעים מתאימים באופן שלא יאפשר איחזור המידע • אין להשתמש בנייר עודף כניירות טיוטה
5.	**שליחה בדואר אלקטרוני**	ללא הנחיות מיוחדות	• העברת המידע בתוך הרשת הארגונית המאובטחת של הארגון • שליחת המידע רק לגורמים בתוך הארגון הזקוקים לו לצורך מילוי תפקידם • שליחת דוא"ל לגורמי חוץ תוך שימוש במערכת להצפנת מיילים • בדיקת נכונות הכתובות למשלוח ורשימת הנמענים בטרם שליחה (במקרה של השלמה אוטומטית של כתובות ושל שימוש באפשרות "השב לכולם") • במשלוח לאדם מידע חסוי על עצמו בדוא"ל לפי בקשתו - יש לקבל את כתובת הדוא"ל	• אסור לשלוח בדוא"ל רגיל • ניתן לשלוח באמצעות כספת וירטואלית או מערכת מאושרת להצפנת מיילים וזאת תוך בקרה לאבטחת המידע בקצוות.

			מראש מהאדם באופן אישי לאחר זיהויו, ולהבהיר לו הסיכונים לפרטיותו בהעברת מידע חסוי בדרך זו.	
.6	**הדפסה**	ללא הנחיות מיוחדות	• הדפסה במדפסת שאינה נגישה לגורמים לא מורשים או הנמצאת במקום הנתון לפיקוח או השגחה. • יש לוודא לקיחת מסמך מהמדפסת מיד בתום ההדפסה • ליד המדפסת יהיה פח למיחזור וגריסה או מגרסה כאמור בפרק על השמדה	• הדפסה במדפסת ייעודית בלבד • המדפסת נמצאת במתחם ממודר שאינו נגיש לציבור ולגורמים לא מורשים • יש לוודא לקיחת מסמך מהמדפסת מיד עם סיום ההדפסה • ליד המדפסת יהיה פח למיחזור וגריסה או מגרסה כאמור בפרק על השמדה
.7	**שליחה בדואר**	ללא הנחיות מיוחדות	• שימוש בדואר ישראל (רגיל) • משלוח במעטפה שהסיווג "חסוי" אינו מסומן עליה • על המעטפה יכתב – "אישי למכותב בלבד" • משלוח במעטפה עליה מצוי המידע המינימלי ההכרחי על השולח, אם יש במידע זה כדי להעיד על תוכן המעטפה • על המעטפה יהיו הוראות	• שימוש בדואר רשום, או דואר שליחים של דואר ישראל, או שליח מקומי, או חברת שליחויות המאושרת על ידי מנהל הביטחון של הארגון. • המעטפה תסומן באמצעות מדבקה ייחודית למוסד השולח, ובה המידע המינימלי ההכרחי על השולח. • שימוש בשיטת מעטפה כפולה – על המעטפה הפנימית יצוין "חסוי ביותר" ועל המעטפה החיצונית לא יצוין סיווג

			בדבר החזרה לשולח במקרה של אי מסירה	אך יכתב – "אישי למכותב בלבד" • על המעטפה יהיו הוראות בדבר החזרה לשולח במקרה של אי מסירה
8.	**שליחה באמצעות מכשיר פקס** **(לעניין פקס ממוחשב יש להתייחס כמו אל דוא"ל)**	ללא הנחיות מיוחדות	• שליחת פקס לאחר וידוא המספר • וידוא קבלת הפקס טלפונית • סימון הפקס באזהרה והודעה על כך שהוא מכיל מידע חסוי, ובקשה ממקבל שאינו הנמען הנכון להודיע לשולח ולהשמיד את הפקס. • במשלוח לאדם מידע על עצמו בפקס לפי בקשתו - קבלת המספר מראש מהאדם באופן אישי לאחר זיהויו, ולהבהיר לו הסיכונים לפרטיותו בהעברת מידע חסוי בדרך זו.	• שליחה ראשונית של פקס: מסמך ריק עליו מצוין "בדיקה" • לאחר אישור קבלת הפקס הראשוני, משלוח החומר החסוי באמצעות **חיוג חוזר** ולא חיוג מחדש של המס'. • וידוא קבלת הפקס טלפונית. • סימון הפקס באזהרה והודעה על כך שהוא מכיל מידע חסוי, ובקשה ממקבל שאינו הנמען הנכון להודיע לשולח ולהשמיד את הפקס. • במשלוח לאדם מידע על עצמו בפקס לפי בקשתו - קבלת המספר מראש מהאדם באופן אישי לאחר זיהויו, ולהבהיר לו הסיכונים לפרטיותו בהעברת מידע חסוי ביותר בדרך זו.
9.	**גישה לאינטרנט**	ללא הנחיות מיוחדות	אסורה הגישה לאינטרנט משרתי אפליקציה ושרתי בסיסי נתונים	• אסורה הגישה לאינטרנט מעמדות המכילות חומר חסוי ביותר או נגישות למערכות חסויות ביותר. • אם אין מנוס יש להבטיח הגנות ברמה גבוהה: מניעת התקנת תוכנות חיצוניות, מניעת הכנסת מדיה נשלפת ,

				בנוסף לאמצעי ההגנה כמו על מידע חסוי
.10	**גישה לאינטרנט עבור שרתים**	ללא גישה לאינטרנט. במידת הצורך באישור ממונה אבטחת מידע	ללא גישה לאינטרנט. במידת הצורך באישור ממונה אבטחת מידע	• אסורה הגישה לאינטרנט מעמדות המכילות חומר חסוי ביותר או נגישות למערכות חסויות ביותר. • אם אין מנוס יש להבטיח הגנות ברמה גבוהה: מניעת התקנת תוכנות חיצוניות, מניעת הכנסת מדיה נשלפת , בנוסף לאמצעי ההגנה כמו על מידע חסוי
.11	**רשת ארגונית**	• ניטור שוטף של הרשת • ביצוע בקרת אירועים חריגים • עדכון שוטף של מערכות ההגנה • ביצוע סקרי סיכונים אחת ל- 36 חודשים	• הגנה על המערכות באמצעות FW ו- FW אפליקטיבי. • ניטור שוטף של הרשת • ביצוע בקרת אירועים חריגים • עדכון שוטף של מערכות ההגנה • ביצוע סקרי סיכונים אחת ל- 24 חודשים	• אם המערכת עצמאית ואין הכרח לקשרה לסביבות אחרות, יש ליישמה בסביבה נפרדת (stand alone) • אם המערכת מחייבת קישור לסביבות אחרות, יש לאפיין תשתיות הגנה מתאימות על הקישור ולקבל אישור מנהל אבטחת המידע בארגון, לצורך החיבור ואופי חיבור המערכת לסביבה האחרת. • חיבור מערכת לרשת יבוצע בסגמנט נפרד וייעודי • הסגמנט הנפרד יאובטח על ידי : ○ firewall ○ Intrusion Prevention) IPS System) שיוטמע לצד ה Firewall ○ Application level firewall שיוטמע גם הוא בסגמנט הנפרד שהוגדר עבור המערכת. • ניטור שוטף של הרשת

				• ביצוע בקרת אירועים חריגים • עדכון שוטף של מערכות ההגנה • ביצוע סקרי סיכונים אחת ל- 24 חודשים
.12	**גישה מרחוק**	ללא הנחיות מיוחדות	• מתבצעת בתווך מוצפן • מתבצעת באמצעות הזדהות דו-שלבית (2 factor authentication)	• אסורה גישה ישירה ! • גישה מרחוק תאושר רק בהתקיים: ○ גישה דו שלבית (באמצעות התקן תוך רשתי) ○ הזדהות חזקה ○ תווך מוצפן ומוקשח ○ אישור הפתרון ע"י ממונה אבטחת מידע במשרד הבריאות
.13	**גיבוי**	ללא הנחיות מיוחדות	• יש לשמור את הגיבוי בכספת חסינת אש • יש למקם את הכספת במקום מרוחק מהמקום בו נמצאות תשתיות המערכת. • מידי חודש יתבצעו בדיקות שחזור לגיבויים	• גיבוי חומר חסוי ביותר יהיה מוצפן • יש לשמור את הגיבוי בכספת חסינת אש, בנפרד משאר הגיבויים המוחזקים באתר • יש למקם את הכספת במקום מרוחק מחדר השרתים בו נמצאות תשתיות המערכת. • מידי חודש יתבצעו בדיקות שחזור לגיבויים
.14	**גישת ספקים מרחוק לרשת**	• רק במקרים נחוצים ובכפוף להסכם עם הספק	• רק במקרים הכרחיים • רק בפיקוח גורם מוסמך מטעם הארגון	אסור

	הארגון	המגדיר את התנאים • רק בפיקוח של גורם מוסמך מטעם הארגון • לא יורשה מצב בו לספק ניתנה גישה ללא הגבלה ופיקוח אל רשת הארגון • הארגון יפתח את תווך ההתחברות של הספק כאשר ההתחברות נדרשת, ובשאר הזמן תווך ההתחברות יהיה חסום • כל התחברות של ספק תהיה מנוטרת ותירשם ללוג של המערכת	• רק לאחר עריכת הסכם עם הספק המגדיר את התנאים, וחתימה של הספק ושל עובדיו על התחייבויות לשמירת סודיות ולהשמדת מידע עודף, והחזרת/השמדת מידע לאחר גמר ההתקשרות • לא יורשה מצב בו לספק ניתנה גישה ללא הגבלה ופיקוח אל רשת הארגון • הארגון יפתח את תווך ההתחברות של הספק כאשר ההתחברות נדרשת, ובשאר הזמן תווך ההתחברות יהיה חסום • כל התחברות של ספק תהיה מנוטרת ותירשם ללוג של המערכת	
15.	**מסירת מידע רגיש**	מסירת מידע לפי חוקים ונהלים	• אסורה מסירת מידע פרטני רפואי למתקשרים בטלפון,	• אסורה

	בטלפון	ספציפיים הרלוונטיים לנושא	למעט במצבי חירום (כגון אר"ן). • ניתן למסור מידע בהתקשרות יזומה מצד המוסר, למספר שנמסר ע"י המקבל. • ניתן לקבל ולמסור מידע ברף הנמוך של רגישות (כגון זימון תורים) לאחר וידוא זהות מקבל המידע בטלפון באמצעי הזדהות שיוגדרו, לפי סוג השירות ולאחר בחינה משפטית פרטנית • זיהוי מרחוק באמצעות שני פריטי מידע שלפחות אחד מהם אינו מופיע במרשם האוכלוסין ואינו מפורסם לציבור בדרך אחרת (כגון בספר הטלפונים)	
.16	**מסירת מידע למטופלים באמצעות אתר אינטרנט / אפליקציה**	בקרה על מהימנות המידע	• לאחר הזדהות מול האתר באמצעות סיסמא ושם משתמש שנמסרו למטופל פנים אל פנים, לאחר שזוהה באמצעות תעודה מזהה הכוללת תמונה • ניתן לקבל ולמסור מידע ברף	• אסורה

			הנמוך של רגישות (כגון תורים) לאחר וידוא זהות מקבל המידע באמצעי הזדהות שיוגדרו, לפי סוג השירות ולאחר בחינה משפטית פרטנית (כגון זימון תורים) • זיהוי מרחוק (כגון לשחזור סיסמא)- רק באמצעות פרטים שמסר המטופל, ושאינם מופיעים במרשם האוכלוסין או בפרסום פומבי אחר	
.17	**מסירת מידע פנים אל פנים**	מסירת מידע לפי חוקים ונהלים ספציפיים הרלוונטיים לנושא	• **למטופל** – לאחר זיהוי באמצעות תעודה מזהה או היכרות קודמת • **לקרוב משפחה** – מותר אם המטופל אישר למסור לו פרטים ולאחר זיהוי באמצעות תעודה מזהה, או להורה של קטין לאחר זיהוי באמצעות תעודה מזהה או היכרות קודמת • **למיופה כוח** – מותר בהצגת ייפוי כח תקף וחתום ע"י עד מהימן (מקור או העתק	• **למטופל** –לאחר זיהוי באמצעות תעודה מזהה • **לקרוב משפחה** – מותר אם המטופל אישר למסור לו פרטים ולאחר זיהוי באמצעות תעודה מזהה או להורה לקטין לאחר זיהוי באמצעות תעודה מזהה • **למיופה כוח** – מותר בהצגת ייפוי כח תקף וחתום ע"י עד מהימן (מקור או העתק מתאים למקור) ולאחר זיהוי באמצעות תעודה מזהה • **לאפוטרופוס** – מותר לאחר הצגת צו אפוטרופסות לגוף (מקור או העתק

			מתאים למקור) ולאחר זיהוי באמצעות תעודה מזהה • **לאפוטרופוס** – מותר לאחר הצגת צו אפוטרופסות לגוף (מקור או העתק מתאים למקור) ולאחר זיהוי באמצעות תעודה מזהה • **לשוטר** – מותר לאחר הצגת צו מתאים (מקור או העתק מתאים למקור) או לפי הוראת דין אחרת (באחריות השוטר לנמק ולספק מקור לסמכות) • **לצד שלישי אחר** – (חברות ביטוח, עורכי דין וכו') – מותר לאחר הצגת כתב ויתור סודיות רפואית הרלוונטי לנושא, וחתום ע"י המטופל ועד (מקור או העתק מתאים למקור), או לאחר הצגת צו בית משפט מנומק (מקור או העתק מתאים למקור). • במקרים אחרים לפי הנחיות נהלים ספציפיים ונוהל בנושא ויתור סודיות	מתאים למקור) ולאחר זיהוי באמצעות תעודה מזהה • **לשוטר** – מותר לאחר הצגת צו מתאים (מקור או העתק מתאים למקור) או לפי הוראת דין אחרת (באחריות השוטר לנמק ולספק מקור לסמכות) • **לצד שלישי אחר** – (חברות ביטוח, עורכי דין וכו') - מותר לאחר הצגת כתב ויתור סודיות רפואית הרלוונטי לנושא וחתום ע"י המטופל ועד (מקור או העתק מתאים למקור), או לאחר הצגת צו בית משפט מנומק (מקור או העתק מתאים למקור) **המתייחס מפורשות לנושא המידע המבוקש**. • במקרים אחרים לפי הנחיות נהלים ספציפיים ונוהל בנושא ויתור סודיות

נוהל סיווג מידע **ISO 27799**		
	מהדורה	2.0
	בתוקף מ	ינואר 2018
	א.8	עמוד 25 מתוך 25