משרד הבריאות – נהלי אבטחת מידע			
פרק א-8	**ניהול נכסים**	מהדורה	**1.0**
שם הנוהל	**סיווג מידע**	בתוקף מ	**יולי 2015**
מספר	**א – 8.2**		**עמוד 1 מתוך 32**

תאריך	מחבר	גרסה	שינוי
1/3/07	רן אדלר	1.0	מסמך ראשוני
1/5/07	יהושע פסין	1.1	עריכה
10/08	יהושע פסין	1.2	הוספת סעיף 6 "שיטה לסיווג מידע"
9/8/09	מורנו נאור	1.3	מספור הנוהל בהתאם לתקן + הוספת סעיפים 5.4.3 + 6.2.
05/02/2012	טליה זמיר יהושע פסין	1.4	התאמה לתקן ISO 27799
22/08/12	טליה זמיר תמיר פלדמן	1.5	התאמה לתקן ISO 27799
30/09/2012	שי אמיר	1.6	אישור הנוהל
29/09/14	גבי פטליס	1.7	שינוי סעיף 5.3 והוספת נספח א' אודות הוראות לטיפול במידע לפי סיווגו
05/05/2015	גבי פטליס	1.8	הגדרת הגנות נדרשות עפ"י רמת הסיווג של המערכת
20/09/2016	גבריאל כהן	1.9	הוספת התייחסות ספציפית לגישה לאינטרנט עבור שרתים
24/9/2016	ראובן אליהו	1.9	תיקוף הנוהל

משרד הבריאות – נהלי אבטחת מידע			
פרק א-8	**ניהול נכסים**	מהדורה	**1.0**
שם הנוהל	**סיווג מידע**	בתוקף מ	**יולי 2015**
מספר	**א – 8.2**		**עמוד 2 מתוך 32**

<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'

1.3. הגדרת הגנות נדרשות על פי רמת הסיווג של המערכת – נספח ב'

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.

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 ב**נספח 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.

5.3 <u>סימון מידע מסווג</u>

5.3.1 מסמך שסווג כ"חסוי" או "חסוי ביותר" יסומן באופן בולט.

5.3.2 סיווג תקליטורים, קלטות ומדיה אחרת, תיעשה ע"י הדבקת מדבקה הכוללת את ציון רמת הסיווג.

5.3.3 מסמכים המופקים ממערכות מידע ממוחשבות, ע"י המערכת עצמה יסווגו באופן אוטומטי.

5.4 <u>שמירת, אחסון, העברת והשמדת מידע מסווג</u>

5.4.1 באחריות כל גורם המטפל במידע לוודא כי המידע שבאחריותו מסווג, מסומן מאוחסן, נשמר, מועבר ומושמד בהתאם לסיווגו.

5.4.2 הנחיות לטיפול במידע בהתאם לסיווגו מפורטות בנספח א' לנוהל זה – "סיווג מידע במערכת הבריאות - הוראות לטיפול במידע לפי סיווגו".

5.4.3 מידע עסקי רגיש (סודות מסחריים / קנין רוחני / כספי), יטופל בהתאם לנוהל אבטחת מידע של משרד הבריאות **א -18.1 התאמה לדרישות שע"פ דין**.

5.4.4 מידע בטחוני : מידע בעל רגישות ביטחונית או מדינית – מסווג ומטופל על פי הנחיות המפורטות בנהלי מסגרת לאבטחת מידע - משרד ראש הממשלה 2005.

5.5 <u>טיפול במערכות מידע חדשות</u>

5.5.1 בעת תכנון מערכת חדשה או שינוי במערכת קיימת יש לקבוע סיווג למערכת מידע.

5.5.2 הסיווג יבוצע לפי הוראות נוהל זה.

5.6 <u>שיטה לסיווג מערכות מידע</u>

5.6.1 כלל האפליקציות בארגון ימופו לתוך טבלה.

5.6.2 הטבלה תכיל נתונים טכניים הנוגעים במערכת כגון :

5.6.2.1 למה משמשת המערכת

5.6.2.2 איזה סוג מידע מכילה

5.6.2.3 כמה משתמשים במערכת

5.6.2.4 האם המערכת היא בעלת ממשקים למערכות אחרות או לאינטרנט

5.6.2.5 בעל המידע (תפקיד)

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

5.6.2.7 האם נתונים מסווגים מוצפנים?

5.6.3 טבלה זו תשמש את המשרד לצרכים הבאים:

5.6.3.1 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.

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

5.6.4 רשימת שאלות בנושאים השונים:

5.6.4.1 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 רפואי של אזרחים?	מערכות האוגרות מידע רפואי פרטני של אזרחים הינן מערכות ברמת סיכון גבוהה על פי חוק הגנת הפרטיות.	1- לא 3- כן- אוגרת מידע של פחות מ 1000 אזרחים. 5- כן- אוגרת מידע של מעל 1000 אזרחים.

משרד הבריאות – נהלי אבטחת מידע			
פרק א-8	**ניהול נכסים**	מהדורה	**1.0**
שם הנוהל	**סיווג מידע**	בתוקף מ	**יולי 2015**
מספר	**א – 8.2**		**עמוד 6 מתוך 32**

.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 לזליגת מידע	1 – המערכת אינה מתוחזקת על ידי גורם חיצוני 3- המערכת מתוחזקת על ידי גורם 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.

5.6.4.2 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

5.6.4.3 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	1- עד 20 ועד בכלל 2- בין 21 - 200 4- בין 201 - 1000

		פגיעה בשלמות הנתונים במערכת.	5- מעל אלף

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

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

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

5.6.4.4.3 אח"כ יבוצע ממוצע משוקלל המגדיר את רמת הסיכון במערכת.

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

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

5.6.4.4.6 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	3	**משקל חיסיון במערכת**	4	**משקל אמינות במערכת**	5

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			

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

5.7 **<u>סימון וטיפול במידע</u>**

5.7.1 סימון המידע המסווג יהיה בהתאם ל**נוהל 7.5.3 בקרת רשומות**

7. **<u>חתימה</u>**

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.

משרד הבריאות – נהלי אבטחת מידע			
פרק א-8	**ניהול נכסים**	מהדורה	**1.0**
שם הנוהל	**סיווג מידע**	בתוקף מ	**יולי 2015**
מספר	**א – 8.2**		**עמוד 12 מתוך 32**

.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 • סוגי מדיה שאינם נייר יש להשמיד באמצעים מתאימים.	• 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, באמצעות מגרסת פתיתים

			באופן שלא יאפשר איחזור המידע • אין להשתמש בנייר עודף כניירות טיוטה	• 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 מראש מהאדם באופן אישי לאחר זיהויו, ולהבהיר לו	• אסור לשלוח בדוא"ל רגיל • ניתן לשלוח באמצעות כספת וירטואלית או מערכת מאושרת להצפנת מיילים וזאת תוך בקרה לאבטחת המידע בקצוות.

			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 בדבר החזרה לשולח במקרה של אי מסירה	• 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 אך יכתב – "אישי למכותב בלבד" • על המעטפה יהיו הוראות בדבר החזרה לשולח במקרה של אי מסירה

משרד הבריאות – נהלי אבטחת מידע			
פרק א-8	**ניהול נכסים**	מהדורה	**1.0**
שם הנוהל	**סיווג מידע**	בתוקף מ	**יולי 2015**
מספר	**א – 8.2**		**עמוד 15 מתוך 32**

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	אמצעי הגנה כגון חומת אש, אנטי וירוס, אנטי SPY.	• 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

משרד הבריאות – נהלי אבטחת מידע			
פרק א-8	**ניהול נכסים**	מהדורה	**1.0**
שם הנוהל	**סיווג מידע**	בתוקף מ	**יולי 2015**
מספר	**א – 8.2**		**עמוד 16 מתוך 32**

.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 : o firewall o IPS (Intrusion Prevention System) שיוטמע לצד ה Firewall o 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 הארגון**	• רק במקרים נחוצים ובכפוף להסכם עם הספק המגדיר את התנאים	• רק במקרים הכרחיים • רק בפיקוח גורם מוסמך מטעם הארגון • רק לאחר עריכת הסכם עם הספק המגדיר את התנאים, וחתימה של הספק ושל עובדיו על התחייבויות לשמירת	אסור

		• 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	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 בטלפון**	מסירת מידע לפי חוקים ונהלים ספציפיים הרלוונטיים לנושא	• אסורה מסירת מידע פרטני רפואי למתקשרים בטלפון, למעט במצבי חירום (כגון אר"ן).	• אסורה

			• 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 הנמוך של רגישות (כגון תורים) לאחר וידוא זהות מקבל המידע באמצעי	• אסורה

			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 מתאים למקור) ולאחר זיהוי באמצעות תעודה מזהה • **לאפוטרופוס** – מותר לאחר הצגת צו אפוטרופסות לגוף	• **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 • **לשוטר** – מותר לאחר הצגת צו מתאים (מקור או העתק מתאים למקור) או לפי

			(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	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

נספח ב'

הגנות ודרישות טכנולוגיות בפיתוח מערכות עפ"י סיווג המידע של המערכת

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

סודר	נושא	בקרות	בלמ"ס	מידע חסוי	מידע חסוי ביותר
.1	**זיהוי ואימות בגישת משתמשים**	למערכות בעלות גישה למידע חסוי ביותר קיימת הזדהות חזקה, חד ערכית, באמצעות אמצעי צד שלישי (Token, Smart card וכו').			**נדרש**
.2		קיימת הגנה מפני חשיפה ושינוי של נתוני הזדהות קשיחים ע"י שימוש בהצפנה מתאימה		**נדרש**	**נדרש**
.3		חשבון משתמש הגישה (אנושי או אפליקטיבי) מוגדר לפי עיקרון - Least Privileges		**נדרש**	**נדרש**
.4		תווך תקשורת בתהליך ההזדהות תמיד מוצפן		**נדרש**	**נדרש**
.5	**מנגנוני הרשאות וניהול הרשאות**	משתמש מקבל את מינימום ההרשאות הדרושות לו כדי לבצע את עבודתו.		**נדרש**	**נדרש**
.6		מערכת ההרשאות פועלת על פי העיקרון: "הכול אסור אלא אם כן הוגדר אחרת".		**נדרש**	**נדרש**
.7		המשתמשים והקבוצות ינוהלו במערכות ההרשאה הסטנדרטיות של הקופה		**נדרש**	**נדרש**

סודר	נושא	בקרות	בלמ"ס	מידע חסוי	מידע חסוי ביותר
.8		נאכפות הרשאות המשתמש בכול גישה לאובייקט, מסך, פעולה, פונקציה, ולא מסתמכים בשום צורה על בדיקות שבוצעו בשלב הזדהות הראשונית של המשתמש		**נדרש**	**נדרש**
.9		ניהול ההרשאות מבוצע ע"י ממשק ייעודי. הממשק מאפשר גמישות ככל הניתן, שינוי ברירות מחדל, ופרמטרים בנושאי אבטחת מידע.		**נדרש**	**נדרש**
.10	**ניהול סיסמאות**	סיסמאות למערכות המכילות מידע חסוי ביותר לא מועברות באמצעות צד שלישי או כטקסט לא מוגן (טקסט גלוי) בדואר אלקטרוני.		**נדרש**	**נדרש**
.11		סיסמאות לא מאוחסנות במערכת המחשב בצורה לא מוגנת והגדרת reversible encryption לא יופעל.		**נדרש**	**נדרש**
.12		חשבון משתמש ננעל לגישה לאחר 5 ניסיונות גישה כושלים.			**נדרש**
.13		חשבון משתמש שננעל משוחרר רק על ידי מנהל רשת ורק לאחר שהוא זיהה באופן ודאי את בעל החשבון.			**נדרש**
.14		סיסמאות הינן באורך של לפחות שמונה (8) תווים, המורכבות מאותיות, מספרים ותווים מיוחדים.		**נדרש**	**נדרש**

סודר	נושא	בקרות	בלמ"ס	מידע חסוי	מידע חסוי ביותר
.15		המערכת מכריחה משתמשים חדשים הנכנסים אליה לשנות את סיסמתם הראשונית לסיסמא העומדת בתקן שנקבע עבור סיסמאות וכן תכפה דרישה לשינוי סיסמא בתדירות של 90 יום לכל סיסמא.		**נדרש**	**נדרש**
.16		המערכת זוכרת 6 סיסמאות אחרונות שהיו בשימוש משתמש. (תלוי תשתית ותלוי מדיניות).		**נדרש**	**נדרש**
.17	**שלימות ואימות נתונים, בדיקות קלטים ופלטים** כולל	בדיקות האימות מתבצעות גם בצד המשתמש וגם בצד השרת.	**נדרש**		**נדרש**
.18		מתקיימות בקרות קלט: בדיקות סוג הקלט – type , האם מסוג מספר, מחרוזת, וכו'	**נדרש**	**נדרש**	**נדרש**
.19		בקרות הקלט: בדיקות לגודל הקלט – ערך max וערך min		**נדרש**	**נדרש**
.20		בקרות הקלט: בדיקת לתבנית הקלט כגון תאריך ושעה.		**נדרש**	**נדרש**
.21		בקרות הקלט: בדיקה לוגית ספציפית כגון בדיקה של מספר תעודת זהות או מספר כרטיס אשראי לפי אלגוריתם קיים	**נדרש**	**נדרש**	**נדרש**
.22		בקרות הקלט: שימוש בשיטות white list ע"י שימוש ב regular expression כאשר רוצים לאפשר סוגי קלט שונים לפי תבניות	**נדרש**	**נדרש**	**נדרש**

סודר	נושא	בקרות	בלמ"ס	מידע חסוי	מידע חסוי ביותר
.23	**סודיות, פרטיות מידע רגיש והצפנה**	קיימת הצפנת תווך ע"י שימוש בפרוטוקולי הצפנה כגון SSL \ VPN \ IPSEC.		**נדרש**	**נדרש**
.24		הצפנת מידע רגיש ברמת המסר מתבצעת כאשר מתבצעת העברה של מידע רגיש ברשת ציבורית ללא הצפנת תווך, או כאשר הצפנת התווך מתבצעת ע"י מחשב שאינו נחשב לבטוח(באזור בטוח).		**נדרש**	**נדרש**
.25		מידע רגיש האגור על גבי בסיס הנתונים מוצפן			**נדרש**
.26		מתבצע שימוש באלגוריתמי הצפנה חזקים סטנדרטיים בלבד כגון AES, RSA וכו', אין שימוש באלגוריתמים שפותחו בצורה עצמית.		**נדרש**	**נדרש**
.27		אין שמירה של מידע רגיש בקובצי הגדרות, קבצים זמניים, cookies, זיכרון מטמון וכו'. במידה ומידע נשמר במקומות אלו באישור חריג, נדרש לממש הצפנת המידע הרגיש		**נדרש**	**נדרש**
.28		במידה ונדרש לשמור סיסמאות משתמשים בבסיס מידע, יש לשמור בצורת hash בלבד.		**נדרש**	**נדרש**
.29	**מנגנוני בקרה ותיעוד**	קיימים מנגנוני בקרה ותיעוד שיבטיחו כי משתמש לא יוכל להתכחש לפעולות שביצע במערכת.		**נדרש**	**נדרש**
.30		שמירת מידע לגבי מי עשה ומה לפי הגדרות זמן מוגדרים מראש	**נדרש**	**נדרש**	**נדרש**

סודר	נושא	בקרות	בלמ"ס	מידע חסוי	מידע חסוי ביותר
.31		שמירת אירועי אבטחה לתקופה של 6 חודשים לפחות.	**נדרש**	**נדרש**	**נדרש**
.32	**מימוש גישה בטוחה לבסיסי נתונים ובכלל**	ממומשת גישה באמצעות Stored Procedures ולא לבצע שאילתות SQL דינאמיות		**נדרש**	**נדרש**
.33		קיימת הגדרת משתמש גישה מסוג Least Privileges והגדרת הרשאות גישה ספציפיות בטבלאות ובסיס נתונים – יצירה, מחיקה, קריאה וכו'	**נדרש**	**נדרש**	**נדרש**
.34	**ניהול Session מאובטח**	שמירת נתוני session בצורה בטוחה במהלך חיי המערכת		**נדרש**	**נדרש**
.35		מניעת האפשרות לבצע Session hijacking ע"י קביעת מופע אחד ויחיד עבור כל משתמש מתחנה של משתמש (כלומר יהיה ניתן לפתוח מספר אפליקציות של משתמש רק אם ההפעלה בוצעה מאותה תחנה, אין לאפשר הפעלה המתבצעת מתחנה נוספת).	**נדרש**	**נדרש**	**נדרש**
.36		האפליקציה תאפשר סגירה של session בצורה מסודרת ונוחה בכל אזור אפליקטיבי בו נמצא המשתמש מיד לאחר ביצוע ההזדהות של המשתמש למערכת. כמו כן יוגדרו פרמטרים לניתוק אוטומטי של המערכת במידה ולא בוצעה בה כל פעילות למשך זמן מוגדר	**נדרש**	**נדרש**	**נדרש**

סודר	נושא	בקרות	בלמ"ס	מידע חסוי	מידע חסוי ביותר
.37		סגירה של session תבטיח כי משתמש לא יוכל לבצע שימוש חוזר במערכת ללא ביצוע הזדהות מלאה מחדש.		נדרש	נדרש
.38	ניהול הגדרות (Configuration Management)	הרצת המערכת תחת חשבון עם רמת ההרשאות הנמוכה ביותר הניתנת.		נדרש	נדרש
.39		הגדרת גישה מאובטחת לביצוע תהליכי אדמיניסטרציה במערכת.		נדרש	נדרש
.40		הגנה על הגדרות המערכת בפני שינויים בלתי מורשים.	נדרש	נדרש	נדרש
.41	מניעת מתקפות אפליקטיביות	XXS	נדרש	נדרש	נדרש
.42		SQL injection	נדרש	נדרש	נדרש
.43		DOS	נדרש	נדרש	נדרש
.44		Buffer Overflow	נדרש	נדרש	נדרש
.45	פיתוח מאובטח	מתחילת תהליך הפיתוח משולב יועץ אבטחת מידע, שמפקח על כל היבטי אבטחת המידע לרבות תכנון, אפיון, עיצוב ופיתוח לפי נהלי פיתוח מאובטח, ביצוע Code Review אבטחתי לרכיבים קריטיים במערכת (כגון: רכיבי זיהוי, רכיבי הרשאות, פעולות קריטיות וכו') וכן ליווי תכנון ויישום הארכיטקטורה במערכת		נדרש	נדרש

סודר	נושא	בקרות	בלמ"ס	מידע חסוי	מידע חסוי ביותר
.46		לפני העלאת האפליקציה לייצור, הספק (במידה ומדובר במערכת המפותחת על ידי ספק חיצוני) או מנהל המערכת (במידה ומפותחת עצמאית\ מוצר מדף) מבצע בדיקות קוד על מנת לאתר פרצות אבטחת מידע. ביצוע בדיקה זו תהיה על ידי גורם צד שלישי בלתי תלוי		**נדרש**	**נדרש**
.47		מתוקנות חולשות אבטחת המידע בהתאם לממצאי הבדיקות במערכת לפני העלאתה לאוויר		**נדרש**	**נדרש**
.48		קיימת הפרדה של סביבות הפיתוח והבדיקות מסביבת הייצור ובכלל זה הגבלת גישה ממפתחים למידע ייצורי		**נדרש**	**נדרש**
.49	**ממשקים**	במידה והמערכת הינה עצמאית ויושבת בסביבה אשר אינה דורשת חיבור לממשקים חיצוניים, ו/או החיבור לממשקים חיצוניים אסורה לפי הנחית בעל המאגר, יש ליישמה בסביבה נפרדת (Alone Stand). סביבה כוללת גישה נפרדת לצרכי תחזוקה, גישה נפרדת לצרכי גיבוי וכו'. תחנות הקצה שיעבדו מול המערכת יהיו מנותקות מכל רשת אחרת ויהיו ייעודיות למערכת			**נדרש**

סודר	נושא	בקרות	בלמ"ס	מידע חסוי	מידע חסוי ביותר
.50	**קישור סביבות**	במידה והמערכת דורשת קישור לסביבות אחרות, קיים אישור ממנהל אבטחת המידע בקופה לצורך עצם החיבור ואופי החיבור של המערכת לסביבה האחרת. במידה והמערכת תחובר לרשת יבוצע הדבר באופן מאובטח			**נדרש**
.51	**סגמנטציה**	הקמת המערכת בסגמנט נפרד ברשת. תחנות הקצה המשתמשות במערכת ישבו בסגמנט זה בלבד. לא מתאפשרת גישה למערכת מכל איזור אחר ברשת הארגון מלבד הסגמנט הייעודי			**נדרש**
.52	**Firewall**	מוטמע Network Fire wall ייעודי המפריד בין הסביבה שהוגדרה עבור המערכת לבין שאר הרשת. רכיב Firewall זה מפריד גם באופן פנימי בין רכיביה השונים של המערכת, כגון בסיס הנתונים, שרת האפליקציה, משתמשי האפליקציה וכו'. סגמנט זה יהיה מוגן על ידי המערכות הבאות: Intrusion Prevention System - IPS - מוטמע לצד ה Firewall. על המערכת לעבוד באופן פרואקטיבי ולחסום\ לדווח על אירועים בזמן אמת כגון על ידי SMS או מייל.		**נדרש**	**נדרש**

סודר	נושא	בקרות	בלמ"ס	מידע חסוי	מידע חסוי ביותר
.53	**Application level Firewall**	מוטמע Application level firewall - בסגמנט נפרד שהוגדר עבור המערכת. מטרתו הינה הגנה בפני מתקפות אפליקטיביות מצד תחנות המשתמשים במערכת.			**נדרש**
.54	**PT**	לפחות אחת לשנה מבוצע ניסיון חדירה מבוקר מכיוון הרשת אל המערכת על מנת לוודא כי המערכת מוגנת מפני חדירת גורמים בלתי מורשים			**נדרש**
.55	**הגבלת גישה**	קיימת הגבלת גישה למערכת משאר הרשת ולתווך הגישה מכיוון המערכת אל העולם דרך שרת Middleware שאינו מחובר לשני הצדדים באופן רציף. השרת המתווך ייזום את הגישה כלפי חוץ ולא להיפך. המערכת תיזום את הגישה לשרת\ים המתווך\ ים			**נדרש**
.56	**חיבור ממשקים**	חיבור לממשקים החיצוניים מבוצע על ידי תווך מוצפן VPN		**נדרש**	**נדרש**
.57	**גישה מרחוק**	תתקיים גישה מרחוק מבוקרת ומאובטחת תחזוקה או עבודה מרחוק למערכות המסווגות בסיווג "חסוי ביותר." בדגש על תווך מוצפן, הזדהות חזקה, בקרה ותיעוד של הפעילות מרחוק.		**נדרש**	**נדרש**

סודר	נושא	בקרות	בלמ"ס	מידע חסוי	מידע חסוי ביותר
.58	**חיווי ובקרה**	קיים מנגנוני חיווי ובקרה על כלל התשתיות המרכיבות את המערכת (שרתים, תחנות, ציוד תקשורת, כלי אבטחת מידע וכו'		**נדרש**	**נדרש**
.59		יש לתעד אירועי אבטחת מידע ובכללם ניסיונות גישה כושלים, גישה לקבצים מסווגים וכו'.		**נדרש**	**נדרש**
.60		יש לשמור את הלוגים הנאספים לתקופה של לפחות 6 חודשים.		**נדרש**	**נדרש**
.61		קיים גיבוי לקבצי הלוג באופן שוטף לתקופה זהה לשאר הגיבויים במערכת		**נדרש**	**נדרש**
.62	**הגנה מפני מתקפות פיזיות מתקפות לוגיות וקוד עוין**	כל השרתים והתחנות במערכת מוגנים על ידי מערכת End Point Security הכוללת לפחות מערכת Anti virus		**נדרש**	**נדרש**
.63		נקודות תקשורת ברשת חסויה ביותר יוקשחו כך שאך ורק מחשבים מוגדרים מראש יוכלו להתחבר אליהן.			**נדרש**
.64	**גיבויים**	הגיבויים המכילים מידע פסיכיאטרי נשמרים באופן מוצפן.			**נדרש**
.65	**עדכוני אבטחה והקשחת המערכת**	מערכות ההפעלה והאפליקציות השונות מעודכנות באופן שוטף בעדכוני האבטחה האחרונים.		**נדרש**	**נדרש**

סודר	נושא	בקרות	בלמ"ס	מידע חסוי	מידע חסוי ביותר
.66		לפני העלאת מערכת המכילה/מקושרת למידע חסוי ביותר לייצור מבוצע תהליך הקשחה של מערכות ההפעלה והתקשורת על פי סטנדרטים מקובלים של הקשחה.		**נדרש**	**נדרש**
.67		כלל השרתים והתחנות נעולים לגישה של התקן מדיה חיצוני (On Disk Key, CD) הן לשמירה והן להעלאה. הנעילה יכולה להיות פיזית או לוגית באחריות הגורם המספק את המערכת לוודא כי לא ניתן לעקוף חסימה זו.			**נדרש**
.68	**שמירת מידע חסוי ביותר על תחנת קצה, מחשב נייד, ומדיה נתיקה**	במידה ומערכת מאפשרת לשמור מידע חסוי ביותר על תחנת קצה, מחשב נייד ו/או מדיה נתיקה- המחשב/ המדיה מוצפן באופן מלא.		**נדרש**	**נדרש**
.69	**היבטי אבטחת מידע פיזיים**	קיימת הגנה פיזית על מערכות הנגישות למידע חסוי ביותר ועל סביבת העבודה .			**נדרש**