


שם הנוהל	ציות והענות			מספר	OPR.11.01.010
מטרות הנוהל	יישום תהליכים מבוקרים, על מנת למנוע הפרות דרישות החוק ו/או דרישות רגולטוריות וכן להבטיח את יישום הוראות מדיניות אבטחת המידע המאושרת ע"י הנהלת מאוחדת, נהלי אבטחת המידע והוראות העבודה השונות.				
סוג הנוהל	חוצה ארגון				
נושא	חטיבת תפעול				
תת-נושא	אבטחת מידע				
כותב הנוהל	משה שחר- ממונה אבטחת מידע				
יחידה אחראית ליישום	ממונה אבטחת מידע				
נדרשים לאשר	סמנכ"ל תפעול, מנכ"ל				
גורמים משתתפים בתהליך	הנהלה, מנכ"ל, סמנכ"לים, ראשי אגפים, מנהלי מחוזות, כלל עובדי מאוחדת				
תאריך כניסה לתוקף	20.7.2014	תאריך בדיקת עדכניות	1.8.2017		
מילות חיפוש	אבטחת מידע				
גרסה	מחות השינוי	תאריך אישור	כותב הגרסה	מאשרי הגרסה	
1.0	חדש	20.7.2014	משה שחר	עוזי ביתן, זאב וורמברנד	

## תוכן העניינים

סעיף	עמוד
כללי	3
מטרות	3
הנוהל חל על	3
הגדרות ומונחים	3
מסמכים ישימים	3
אחריות וסמכות	4
שיטה	5
חריגים	14
בקרה ודיווח	14
רשימת הוראות עבודה נגזרות	14

 <b>מאוחדת</b> להיות בריא ולהישאר בריא	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך: 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 2 מתוך 14		שם הנוהל: ציות והענות	

## 1. כללי

אי ציות ו/או הפרות של חוקים, הוראות ותקנות ומדיניות אבטחת מידע עלולים לשבש את הפעילות השוטפת של הארגון ולחשוף אותו לאי יכולת לספק שרות, תביעות משפטיות ופגיעה קשה בתדמית.

## 2. מטרת

- 2.1. יישום תהליכים מבוקרים על מנת למנוע הפרות של דרישות החוק ו/או דרישות רגולטוריות.
- 2.2. הבטחת יישום הוראות מדיניות אבטחת המידע המאושרת ע"י הנהלת מאוחדת, נהלי אבטחת המידע והוראות העבודה השונות.

## 3. הנוהל חל על

ההנהלה, סמנכ"לים, מנהלי מחוזות, מנהלי אגפים ומנהלי תחומים במטה ובמחוזות, בעלי מידע, אגף מערכות מידע.

## 4. הגדרות ומונחים


- 4.1. **חוק הגנת הפרטיות**: חוק מדינה המגדיר כהפרת חוק מקרה של גילוי פרטים אישיים של אדם, ללא אישורו.
- 4.2. **תקן ISO 27799**: תקן בינלאומי המגדיר את תהליכי ניהול אבטחת מידע בארגוני בריאות. משרד הבריאות מחייב את כל ארגוני הבריאות בישראל להטמיע תקן זה.
- 4.3. **תקן PCI DSS**: ביוזמת חברות כרטיסי האשראי הבינלאומיות נוצר תקן בינלאומי המחייב את כל העסקים הסולקים כרטיסי אשראי, להטמיע דרישות אבטחת מידע מחמירות.
- 4.4. **מסמך מדיניות אבטחת מידע**: מסמך יזום ומאושר ע"י הנהלת הקופה המגדיר את תהליכי הבקרה של מדיניות אבטחת המידע במאוחדת.
- 4.5. **נוהל אבטחת מידע**: הנחיה מחייבת מתוקף מסמך מדיניות אבטחת מידע, לתהליכים ליישום מדיניות אבטחת המידע.
- 4.6. **הוראות עבודה**: הנחיה מקצועית מחייבת מתוקף נוהל אבטחת מידע ספציפי.

## 5. מסמכים ישימים

- 5.1. חוק הגנת הפרטיות – ה'תשמ"א, 1981, כולל התיקונים שאושרו ע"י הכנסת והתקנות שהותקנו ע"י שר המשפטים.
- 5.2. חוק הגנת הפרטיות – ה'תשמ"א, 1981, כולל התיקונים שאושרו ע"י הכנסת והתקנות שהותקנו ע"י שר המשפטים.
- 5.3. חוק המחשבים, ה'תשנ"א, 1995, כולל התיקונים והשינויים שאושרו ע"י הכנסת.
- 5.4. חוק ביטוח בריאות ממלכתי, ה'תשנ"ד, 1994, כולל התיקונים והשינויים שאושרו ע"י הכנסת והממשלה.

### לשימוש פנימי בלבד

זכויות יוצרים "מאוחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאוחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאוחדת.

 <b>מאחדת</b> להיות בריא ולהישאר בריא	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך: 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 3 מתוך 14		שם הנוהל ציות והענות	

5.5. חוק זכויות החולה – ה'תשנ"ו – 1996.

5.6. חוק יסוד כבוד האדם וחירותו, ה'תשנ"ד, 1994, כולל התיקונים והשינויים שאושרו ע"י הכנסת.

5.7. תקן מ"י ISO 27799

5.8. תקן מ"י ISO 27002

5.9. תקן PCI DSS (Pay Card Industries Data Security Standard)

5.10. תקנות iSOX של הרשות לניירות ערך.

5.11. מדיניות אבטחת מידע במאוחדת.

## 6. אחריות וסמכות

6.1. הממונה על אבטחת מידע

6.1.1. אחראי ליישום ואכיפתו של נוהל זה, בהתאם למדיניות אבטחת המידע.


6.1.2. דווח להנהלת מאוחדת במקרה של הפרה חלקית או מלאה של נוהל זה.

### לשימוש פנימי בלבד

זכויות יוצרים "מאוחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאוחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או

להפצה ו/או להעתיקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאוחדת.



 <p>מאוחדת להיות בריא ולהישאר בריא</p>	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך: 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 4 מתוך 14		שם הנוהל: ציות והענות	

## 6.2. הנהלת מאוחדת

6.2.1 קביעת האמצעים המשמעותיים במקרה של הפרה חלקית או מלאה של נוהל זה, על פי דיווח הממונה על אבטחת המידע, ובהתאם למדיניות אבטחת המידע במאוחדת.

## 7. שיטה

### 7.1. ציות לדרישות חוק

במטרה למנוע הפרות של חוקי מדינת ישראל, תקנות ממשלתיות ותקנים בינלאומיים, דרישות רגולטוריות בישראל והתקשרויות חוזיות עם גורמים חיצוניים, ועל מנת לשמר מדיניות אבטחת מידע נאותה יש לפעול כדלקמן.

#### 7.1.1. זיהוי חקיקה רלוונטית


א. באחריות הממונה על אבטחת מידע ובשיתוף עם היועץ המשפטי לנהל, לשמר ולעדכן באופן שוטף, קובץ מידע עם כל הרכיבים הישימים לסביבת העבודה במאוחדת, לפי הפרטים שלהלן:

- 1) חוקים – חוק הגנת הפרטיות, חוק זכויות החולה, חוק יסוד כבוד אדם וחירותו, חוק המחשבים, חוק ביטוח בריאות ממלכתי, חוק הארכיונים.
  - 2) תקנות ודרישות רגולטוריות – תקנות משרד הבריאות, תקנות משרד האוצר, חוזרי מנכ"ל משרד הבריאות (הישימים לאבטחת מידע ומערכות מידע), תקנים (ראה סעיף הבא).
  - 3) תקנים בינלאומיים – PCI DSS, ISOX, ISO 27001, ISO 27002, ISO 27799.
  - 4) התקשרויות חוזיות – בתי חולים, משרדי ממשלה, ספקי ציוד, ספקי שרות, ספקי תקשורת, ספקי תוכנה.
- ב. חובה לכלול בכל מסמך נוהל ו/או הוראות עבודה, פרק "מסמכים ישימים", הישימים ורלוונטיים לאותו מסמך.
- ג. באחריות הממונה על אבטחת מידע לקיים הליך קבוע, במסגרת ביקורות אבטחת המידע השוטפות, בו יש לבדוק את תאימות המערכת הנבדקת ליישום ההוראות במסמכים הישימים.
- ד. באחריות מבקר פנים לקיים הליך קבוע. בו יש לבדוק את תאימות המערכת המבוקרת ליישום ההוראות במסמכים הישימים.

### לשימוש פנימי בלבד

זכויות יוצרים "מאוחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאוחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או

להפצה ו/או להעתיקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאוחדת.

 <b>מאוחדת</b> להיות בריא ולהישאר בריא	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך : 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 5 מתוך 14		שם הנוהל ציות והענות	


#### ה. קניין רוחני

- 1) הגדרות קניין רוחני:
  - 2) סוד מסחרי – Trade Secret
  - 3) סימן רשום – Trade Mark
  - 4) זכות יוצרים – Copyright
  - 5) פטנט – Patent
- ו. באחריות היועץ המשפטי לגבש כללי אתיקה, לאישור ההנהלה, ובהם הנחיות לכל היחידות הארגוניות כיצד לנהוג בסוגיות קניין רוחני כמפורט בסעיף לעיל, תוך ציון אמצעי הענשה הצפויים להפרות של כללי האתיקה בנושא קניין רוחני.
  - ז. באחריות היועץ המשפטי לגבש הנחיות, לאישור ההנהלה, כיצד לנהוג בקניין רוחני שבבעלות מאוחדת.
  - ח. חל איסור להפר זכות יוצרים של מוצרי תוכנה, חומרה, תקשורת ואביזרים נלווים.
  - ט. רכישת מוצרים (כמפורט בסעיף לעיל) חובה לבצע רק ממשווקים מורשים או מהימנים. חובה לצרף לכל רכישה הסכם רישוי מטעם המשווק/יצרן.
  - י. עם רכישת מוצר תוכנה, באחריות ראש אגף מערכות מידע להנחות על שמירה, במקום מאובטח, של התקליטור המקורי של התוכנה והספרות הנלווית.
  - יא. באחריות ראש אגף מערכות מידע למנות מתוך אגף מערכות מידע, גורם שאחראי לניהול רישוי התוכנה בכל רבדי הארגון.
  - יב. באחריות הגורם האחראי לניהול הרישוי, לקיים באופן שוטף, תהליכים לסריקת שימוש בתוכנה, באמצעי טכנולוגי מתאים, על מנת לבקר את התאמת השימוש בתוכנה עם הסכמי הרישוי.
  - יג. במקרה ונמצאו אי התאמות באופן השימוש בתוכנה לעומת הסכמי הרישוי, חובה על הגורם האחראי לניהול הרישוי, לדווח אל ראש אגף מערכות מידע.
  - יד. באחריות הגורם האחראי לניהול הרישוי, לתעד בקובץ ייעודי, את כל הסכמי הרישוי התקפים לרכישת תוכנה.

#### לשימוש פנימי בלבד

זכויות יוצרים "מאוחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאוחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתיקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאוחדת.




 <b>מאוחדת</b> להיות בריא ולהישאר בריא	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך : 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 6 מתוך 14		שם הנוהל ציות והענות	

### 7.1.2. הגנה על רשומות ארגוניות

- א. חובה לשמור רשומות ארגוניות לתקופות המוגדרות על פי הוראות החוק והתקנות. כמו כן יש לשמור רשומות ארגוניות לצורך ביצוע תחקורים לאחר על פי הצורך ודרישה.
- ב. חובה לקיים מדיניות אבטחת מידע על מנת לקיים הגנה נאותה על הרשומות הארגוניות הכוללת, הגנה קפדנית על בסיסי נתונים וקבצים, בקרת גישה קפדנית ולמורשים בלבד, אחסון מידע באופן מאובטח.
- ג. רשומות ארגוניות שמורות ואגורות בהתאם לשתי התצורות הבאות:
- 1) רשומות ארגוניות במערכת המחשב (אלקטרוני) – בסיסי נתונים, קבצים.
  - 2) רשומות ארגוניות כמידע פיזי – קלט מחשב, מדיה אופטית.
- ד. חובה לקטלג, בעת שמירה של רשומות ארגוניות, על פי המגזרים הבאים:
- 1) מידע רפואי
  - 2) מידע פיננסי
  - 3) מידע מנהלתי
- ה. רשומות ארגוניות במערכת מחשב
- 1) רשומות ארגוניות בסביבת התפעול של המחשב המרכזי מקוטלגות, ישמרו בהתאם לסף הקיבולת האפשרי בסביבת התפעול, או לפרק הזמן שלא יעלה על 3 שנים.
  - 2) במידה וסף הקיבולת של הסביבה התפעולית של המחשב המרכזי הגיעה לספה או עברו 3 שנים שרשומות ארגוניות אגורות בסביבה התפעולית, יש לקיים, באחריות מנהל התוכנה באגף מערכות מידע, תהליך אוטומטי של העברת הרשומות אל מחיצה אחרת במחשב המרכזי (History).
  - 3) רשומות ארגוניות האגורות במחיצת History לא יוגבלו בסף קיבולת ובפרק זמן של אגירה.
  - 4) באחריות מנהל התוכנה באגף מערכות מידע להנחות על פיתוח אמצעי חיפוש טכנולוגיים, הן בסביבה התפעולית והן במחיצת History, לשליפת מידע באופן אופטימאלי ועל פי הצורך.
  - 5) במידה ונדרשת שליפת מידע מהרשומות הארגוניות, בסביבה התפעולית או ממחיצת History, יעשה רק על פי דרישה של מי ממוסדות המדינה המוסמכים (בתי משפט, רשות המיסים, משרדי ממשלה) ו/או לצורך תחקור הונאה ו/או לצורך תחקור אירוע אבטחת מידע. שליפת רשומות במערכת המחשב תיעשה על דעת

#### לשימוש פנימי בלבד

זכויות יוצרים "מאוחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאוחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתיקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאוחדת.

 <b>מאוחדת</b> להיות בריא ולהישאר בריא	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך: 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 7 מתוך 14		שם הנוהל ציות והענות	

מנהלי היחידות הארגוני הרלוונטיות למידע המקוטלג.

1. רשומות ארגוניות כמידע פיזי
  - (1) רשומות ארגוניות כמידע פיזי ישמרו בארכיונים לפרקי הזמן כפי שנקובים בחוק הארכיונים, על פי הקטלוג של המידע
  - (2) באחריות סמנכ"ל תפעול למנות גורם אחראי, מתוך חטיבת התפעול, האחראי על ניהול תהליכי הארכוב והגניזה של רשומות ארגוניות כמידע פיזי, בכל היחידות הארגוניות.
  - (3) באחריות הממונה על אבטחת מידע לגבש הוראת העבודה המסדירה את תהליכי האיסוף, הארכוב והגניזה של רשומות ארגוניות כמידע פיזי.
  - (4) רשומות ארגוניות כמידע פיזי הנדרשות לשמירה, אך לא בארכיון, יעשה כן בהתאם להוראות מנהל היחידה הארגונית הרלוונטית באופן מאובטח ובהתאם לכללי אבטחת המידע (ראה חוברת "כללי אבטחת מידע לעובד").
  - (5) רשומות ארגוניות כמידע פיזי (פלטי מחשב) מסווגות, ולא נדרשות לשמירה או ארכוב, יש להשמיד
  - (6) רשומות ארגוניות כמידע פיזי (תקליטורים) עם מידע מסווג, ולא נדרשות לשמירה או ארכוב, יש להשמיד


### 7.1.3 הגנה על המידע ופרטיות המידע האישי

- א. על מנת לקיים הגנה הדוקה על הפרטיות, על מידע המסווג "חסוי אישי" (בכפוף להוראות נוהל על "ניהול נכסי מידע") חובה לאכוף מדיניות אבטחת מידע הממוקדת לטיפול בסוג מידע זה.
- ב. באחריות הממונה על אבטחת המידע לקבוע את הבקורות הנדרשות לאכיפת מדיניות אבטחת המידע הממוקדת
- ג. באחריות הממונה על אבטחת המידע, לקיים לכל הפחות אחת לשנה, תהליך מתועד של הערכת סיכונים במידע המסווג כ"חסוי אישי" ולעדכן את מדיניות אבטחת המידע הממוקדת בהתאם לממצאי הערכת הסיכונים.
- ד. מידע "חסוי אישי" מזוהה על פי מגזרי הפעילות הבאים:

#### לשימוש פנימי בלבד

זכויות יוצרים "מאוחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאוחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאוחדת.




 <p>מאחדת לחיות בריא ולהישאר בריא</p>	גרסה 1.0	מספר הנוהל OPR.11.01.010	יחידה ארגונית אחראית ליישום: ממונה על אבטחת מידע
	בתוקף מתאריך : 20.7.2014		נושא: חטיבת תפעול
	סטטוס: מאושר		תת נושא: אבטחת מידע
דף 8 מתוך 14		שם הנוהל ציות והענות	

- (1) "חסוי אישי" רפואי – "מידע בריאות אישי" בהתאם להגדרת ISO 27799, מידע רפואי אישי של המטופלים במאוחדת.
- (2) "חסוי אישי" פיננסי – מידע פיננסי פרטי של לקוחות מאוחדת.
- (3) "חסוי אישי" מנהלתי – מידע אישי של עובדי מאוחדת (על פי הגדרות נוהל על "אבטחת מידע במשאבי אנוש")
- (4) מידע בריאות אישי – הנחיות
- (א) חל איסור לראות ו/או לחשוף מידע בריאות אישי של מטופל, ללא הרשאת המטופל והסכמתו הכתובה לכך.
- (ב) הרשאות גישה למידע בריאות אישי יונפקו על פי "הצורך לדעת" ולפי הגבלות הגדרת התפקיד ובכפוף להוראות נוהל על "בקרת גישה".
- (ג) חל איסור לשלוח מידע בריאות אישי באמצעות מכשירי פקסימיליה, גם לצורכי עיבוד פנים ארגוניים.
- (ד) משלוח מידע בריאות אישי לצורכי עיבוד פנים ארגוניים באמצעות דואר אלקטרוני, יעשה באופן מאובטח משלוח מידע בריאות אישי באמצעות דואר ישראל ו/או דואר אלקטרוני יעשה רק בהסכמה מפורשת של המטופל, בעל המידע בריאות אישי או על פי דרישות החוק.
- (6) מסירת מידע בריאות אישי באמצעות שיחת טלפון או מרכז שירות (Call Center) ו/או חשיפת מידע בריאות אישי לארגון שמחוץ למאוחדת, יעשה רק בהסכמה מפורשת של המטופל, בעל המידע בריאות אישי או על פי דרישות החוק.
- (7) פרסום מידע בריאות אישי באתר האינטרנט של מאוחדת יעשה באמצעות "מאוחדת און ליין" תוך הקפדה חמורה על גישה למידע על מטופל ע"י המטופל עצמו בלבד.
- (8) חל איסור לפרסם מידע בריאות אישי באתר האינטרא-נט (פורטל).
- ה. חסוי אישי פיננסי
- (1) חל איסור לראות ו/או לחשוף מידע חסוי אישי פיננסי של לקוחות, ללא הרשאתו הכתובה והסכמתו לכך.
- (2) הרשאות גישה למידע חסוי אישי פיננסי יונפקו על פי "הצורך לדעת" ולפי הגבלות הגדרת התפקיד ובכפוף להוראות נוהל על "בקרת גישה".
- (3) חל איסור לשלוח מידע חסוי אישי פיננסי באמצעות מכשירי פקסימיליה, גם לצורכי עיבוד פנים ארגוניים.
- לשימוש פנימי בלבד

זכויות יוצרים "מאוחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאוחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאוחדת.



 <b>מאוחדת</b> להיות בריא ולהישאר בריא	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך: 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 9 מתוך 14		שם הנוהל ציות והענות	


- 4) חל איסור לשלוח מידע חסוי אישי פיננסי באמצעות דואר ישראל ו/או דואר אלקטרוני.
- 5) חל איסור למסור מידע חסוי אישי פיננסי באמצעות שיחות טלפון ו/או מרכזי שירות (Call Center) ו/או לחשוף מידע חסוי אישי פיננסי לארגון שמחוץ למאוחדת מלבד דרישה מוסמכת מרשויות החוק בלבד.
- 6) טיפול בפרטי כרטיסי אשראי – על פי דרישות תקן PCI DSS חלה חובה לשמור ולטפל בפרטי כרטיסי אשראי, על פי שלושת החלופות שלהלן:
- א) שימוש בהצפנה וניהול מפתחות הצפנה מתאים.
- ב) החלפת הנתון של פרטי כרטיס אשראי בToken ייעודי.
- ג) ביצוע פעולת Hash על הנתון פרטי כרטיס אשראי.
- 7) באחריות הממונה על אבטחת מידע לגבש הנחיות עבודה לתפעול פעילות כרטיסי האשראי על דרישות תקן PCI DSS.
- 8) חל איסור לפרסם מידע חסוי אישי פיננסי באתר האינטרנט והאינטרא-נט.

#### 7.1.4. מידע חסוי אישי מנהלתי

- א. חל איסור לראות ו/או לחשוף מידע חסוי אישי מנהלתי של עובדים, ללא הרשאה כתובה מהעובד והסכמתו לכך.
- ב. הרשאות גישה למידע חסוי אישי מנהלתי יונפקו על פי "הצורך לדעת" ולפי הגבלות הגדרת התפקיד ובכפוף להוראות נוהל על "בקרת גישה".
- ג. חל איסור לשלוח מידע חסוי אישי מנהלתי באמצעות מכשירי פקסימיליה, גם לצורכי עיבוד פנים ארגוניים.
- ד. חל איסור לשלוח מידע חסוי אישי מנהלתי באמצעות דואר ישראל, אלא רק באמצעות הדואר הפנימי של מאוחדת.
- ה. משלוח מידע חסוי אישי מנהלתי לצורכי עיבוד פנים ארגוניים באמצעות דואר אלקטרוני, יעשה באופן מאובטח ובכפוף להוראות נספח 10.2 "אבטחת נכסי מידע לפי סיווג – נוהל על "ניהול נכסי מידע".
- ו. תהליכי עיבוד השכר של כלל העובדים, המתקיים באמצעות חברה חיצונית (לשכת שרות), יעשה בהקפדה על מדיניות אבטחת מידע בכל הנוגע לשמירת קבצים, מידור הגישה לקבצים וממשקי קישור למערכות מאוחדת.

#### לשימוש פנימי בלבד

זכויות יוצרים "מאוחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאוחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתיקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאוחדת.

 <b>מאחדת</b> להיות בריא ולהישאר בריא	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך: 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 10 מתוך 14		שם הנוהל ציות והענות	

- ז. באחריות הממונה על אבטחת המידע לבצע בקרה שוטפת לגבי מדיניות אבטחת המידע הנהוגה בהתקשרות עם החברה החיצונית שמעבדת את נתוני שכר העובדים ובכפוף להוראות פרק 7.2 "ניהול התקשרויות עם ספקי שירותים צד ג'" – נוהל על ניהול תקשורת ותפעול.
- ח. משלוח תלושי השכר לעובדים חובה לבצע באמצעות דואר פנימי בלבד.
- ט. תהליכי עיטוף תלושי השכר של כלל העובדים, המתקיים באמצעות חברה חיצונית, יעשה בהקפדה על מדיניות אבטחת מידע בכל הנוגע להעברת הקבצים לחברה החיצונית והתחייבות החברה החיצונית לשמירת סודיות.
- י. באחריות הממונה על אבטחת המידע לבצע בקרה שוטפת על החברה החיצונית המבצעת את עיטוף תלושי השכר של העובדים ובכפוף להוראות פרק 7.2 "ניהול התקשרויות עם ספקי שירותים צד ג'" – נוהל על "ניהול תקשורת ותפעול.
- יא. חל איסור לפרסם מידע חסוי אישי מנהלתי באתר האינטרנט.
- יב. פרסום מידע חסוי אישי מנהלתי באתר האינטרא-נט (פורטל) תוך הקפדה על בקרת גישה המבטיחה שמידע אישי של העובד ייראה ע"י העובד בלבד.


#### 7.1.5. מניעת ניצול לרעה של מידע

- א. מידע משמש לביצוע תהליכים ארגוניים בהתנהלות השוטפת של מאוחדת.
- ב. מערכות המידע לסוגיהן, משמשות תשתית לשימוש במידע בתהליכים ארגוניים.
- ג. חל איסור לעשות שימוש באופן זדוני במידע המופק במערכות המידע לסוגיהן, על פי ההגדרות שלהלן:
- (1) שימוש בהרשאות גישה למערכות מידע על מנת לראות, לחשוף, לשנות מידע אישי כגון: מידע רפואי, מידע פיננסי, מידע פרטי, וזאת על מנת לפגוע ולהזיק למטופל, לקוח, עמית לעבודה, וכן לפגוע בתדמיתה ובמהלכיה של מאוחדת.
  - (2) שימוש בהרשאות גישה למערכות מידע על מנת לראות, לחשוף, לשנות מידע ארגוני כגון: מידע רפואי, מידע פיננסי, מידע עסקי, וזאת על מנת לפגוע ולהזיק לעמיתים לעבודה, לקוחות, ספקים וכן לפגוע בתדמיתה ובמהלכיה של מאוחדת.
  - (3) שימוש בהרשאות גישה למערכות מידע על מנת להעתיק, ללא רשות, מידע ארגוני כגון: מידע רפואי, מידע פיננסי, מידע עסקי.

#### לשימוש פנימי בלבד

חכיויות יוצרים "מאוחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאוחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להענתקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאוחדת.



 <p><b>מאוחדת</b> להיות בריא ולהישאר בריא</p>	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך: 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 11 מתוך 14		שם הנוהל ציות והענות	

- 4) שימוש בדואר האלקטרוני הארגוני על מנת להפיץ, ללא רשות, מידע רפואי, מידע פיננסי, מידע עסקי, וזאת על מנת לפגוע ולהזיק לעמיתים לעבודה, לקוחות, ספקים וכן לפגוע בתדמיתה של מאוחדת.
- 5) שימוש בדואר האלקטרוני הארגוני על מנת להפיץ חומרי תועבה, תעמולה פוליטית, פעילות מסחרית לא חוקית.
- 6) שימוש בקלטיים של מחשב, תקליטורים, מדיה נתיקה על מנת לראות, לחשוף ולהפיץ, ללא רשות, מידע רפואי אישי, מידע פיננסי, מידע עסקי.
- ד. באחריות הממונה על אבטחת המידע לגבש אמצעי תיעוד, פיקוח ובקרה, על מנת לבצע ניטור של הפעילויות, המתוארות בסעיף 7.1.5.3 לעיל, בכל פעם שמתעורר חשש לביצוע פעולה מסוג זה.
- ה. באם מתעורר חשש כמתואר בסעיף לעיל, רשאי הממונה על אבטחת מידע לקיים בקרה על פעילות משתמשים, מערכות מידע, שרת דואר אלקטרוני ותחנת עבודה של משתמש, בנוכחותו של המשתמש.
- ו. במקרה וקיימים ממצאים המאמתים את החשש, חובה על הממונה על אבטחת מידע לעדכן את מנהל היחידה הארגונית הרלוונטית למקרה וליזום דיון בוועדת ההיגוי לאבטחת מידע להמשך טיפול עד ההעברה להנהלה.

#### 7.1.6. הסדרת שימוש בהצפנה על פי הדרישות


- א. השימוש באמצעי הצפנה יעשה בהתאמה מלאה לדרישות, המתפרסמות מעת לעת, של הרשות לאבטחת מידע (רא"מ) במשרד ראש הממשלה בישראל.
- ב. ניהול מפתחות ההצפנה יעשה על פי הפרקטיקה המקובלת בכל הארגונים ובהתאמה למדיניות אבטחת המידע של מאוחדת ובהתאם לדרישות רא"מ.
- ג. באחריות הממונה על אבטחת המידע לקיים בקרה שוטפת על דרישות אמצעי הצפנה כמוזכר בסעיפים 7.1.6.1 ו 7.1.6.2 לעיל.
- ד. חל איסור לעשות שימוש באמצעי הצפנה בהתאם לדרישות רא"מ ולדרישות חוקיות הקיימות במדינות אחרות אשר הינן המקור של אמצעי ההצפנה.

#### 7.2. ציות והיענות למדיניות ונהלים

- במטרה להבטיח את תפעול מערכות המידע התומכות בכל התהליכיים הארגוניים, בהתאם למדיניות אבטחת המידע, נהלי העל, הנחיות העבודה וכללי אבטחת המידע במאוחדת, יש לפעול כדלקמן:
- 7.2.1. ביקורת ציות למדיניות ולנהלי על

#### לשימוש פנימי בלבד

חזיונות יוצרים "מאוחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאוחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתיקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאוחדת.


 <b>מאחדת</b> להיות בריא ולהישאר בריא	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך: 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 12 מתוך 14		שם הנוהל ציות והענות	

- א. הגורמים הניהוליים שלהלן אחראים לגיבוש תכנית אכיפה שנתית מתועדת הכוללת בדיקת התאמה וציות של המערכות ותהליכים שתחת אחריותם/ניהולם, למדיניות אבטחת המידע, לנהלי העל ולהנחיות העבודה:
- (1) ההנהלה – באמצעות מבקר פנים
  - (2) ממונה על אבטחת המידע
  - (3) בעלי המידע –
  - (4) אגף מערכות מידע – ראש האגף, מנהל תוכנה, מנהל אבטחת מידע, מנהל תשתיות, מנהל תקשורת.
  - (5) קב"ט ארצי
- ב. באחריות הממונה על אבטחת המידע לרכז את ממצאי בדיקות ההתאמה והציות מכל הגורמים הניהוליים.
- ג. בהסתמך על ממצאי בדיקות ההתאמה והציות, באחריות הממונה על אבטחת המידע לגבש תכנית טיפול באי התאמות ו/או הפרות ציות, בהתאם לעקרונות שלהלן:
- (1) הגדרה מדויקת של המקרים של אי התאמה ו/או הפרת ציות לעומת ההוראות במדיניות אבטחת המידע, נהלי העל והנחיות העבודה.
  - (2) גיבוש פעולות תיקון כגון הדרכה והנחיה, על מנת להבטיח שמקרים של אי התאמה ו/או הפרת ציות לא יחזרו.
  - (3) בקרה שוטפת לגבי ביצוע פעולות התיקון והטמעתם.
- ד. באחריות הממונה על אבטחת המידע, להביא לדיון ולדווח לוועדת ההיגוי לאבטחת מידע את ממצאי בדיקות האי התאמה ו/או הפרות ציות יחד עם תכנית הטיפול.
- 7.2.2 ביקורת ציות טכנית
- א. באחריות הממונה על אבטחת המידע, ליזום ולקיים תהליך שוטף של ביקורת ציות טכנית על מערכות המידע, כולל מערכות במופעלות ע"י גורמי צד ג' או מופעלות באתרים שמחוץ למאחדת, על מנת להבטיח את תפקודם של מערכות אלו בהתאמה לדרישות אבטחת המידע של המדיניות ונהלי על של מאחדת.
- ב. ביקורת ציות טכנית ניתן לבצע בדרכים שלהלן:

#### לשימוש פנימי בלבד

זכויות יוצרים "מאחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאחדת.



 <b>מאחדת</b> להיות בריא ולהישאר בריא	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך: 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 13 מתוך 14		שם הנוהל ציות והענות	


- (1) בקורות ידניות – ביצוע ע"י הממונה על אבטחת המידע או גורם שהורשה ע"י הממונה על אבטחת המידע.
  - (2) שימוש באמצעים טכנולוגיים כגון סורקים או אמצעי ניטור - ביצוע ע"י הממונה על אבטחת המידע או גורם שהורשה ע"י הממונה על אבטחת המידע.
  - (3) הפעלה של גורמים חיצוניים (צד ג') לשם ביצוע סקירות וסקרים, כולל ע"י הפעלה של אמצעים טכנולוגיים (באישור הממונה על אבטחת המידע).
- ג. במקרה של שימוש באמצעים טכנולוגיים לשם ביצוע ביקורת ציות טכנית, חובה להבטיח שפעולה זו אינה פוגעת בתהליכים השוטפים של מערכות המידע, לכן חובה לדמות סביבת ניסוי לפני ביצוע פעולה בסביבה התפעולית.
- ד. באחריות הממונה על אבטחת המידע להכין תכנית ביקורת ציות טכנית, הכוללת את האמצעים לביצוע הביקורת (תכנית ביקורת הציות הינה חלק מתכנית העבודה השנתית של הממונה על אבטחת המידע כפי שמוצגת בפני וועדת ההיגוי לאבטחת מידע.
- ה. במקרה ואם בביקורת הציות הטכנית, ישנם ממצאים המצביעים על אי התאמה של מערכות מידע לדרישות אבטחת המידע, באחריות הממונה על אבטחת המידע, בתיאום עם ראש אגף מערכות מידע וכל הגורמים הרלוונטיים באגף מערכות מידע, להכין תכנית טיפול בליקויים הכוללת פעולות תיקון ו/או שינוי במערכות המידע הרלוונטיות.
- ו. באחריות הממונה על אבטחת המידע לדווח על תכנית טיפול הליקויים לבעלי המידע הרלוונטיים ולקיים דיון על תכנית הטיפול בפני וועדת ההיגוי לאבטחת מידע.

## 8. חריגים

אין חריגים לנוהל

### לשימוש פנימי בלבד

זכויות יוצרים "מאחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתיקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאחדת.

 <b>מאחדת</b> להיות בריא ולהישאר בריא	גרסה	מספר הנוהל	יחידה ארגונית אחראית ליישום:
	1.0	OPR.11.01.010	ממונה על אבטחת מידע
	בתוקף מתאריך : 20.7.2014		נושא: חטיבת תפעול
		סטטוס: מאושר	תת נושא: אבטחת מידע
דף 14 מתוך 14		שם הנוהל ציות והענות	

## 9. בקרה ודיווח

- 9.1. הממונה על אבטחת המידע אחראי על ביצוע בקרה שוטפת של כל מרכיבי נוהל זה. במסגרת הסקירה השנתית לגבי מצב אבטחת המידע במאחדת באחריות הממונה על אבטחת המידע למסור, בפני ועדת היגוי לנושאי אבטחת מידע, דיווח מפורט על ביקורת ביצוע של נוהל זה.
- 9.2. אחריות הממונה על אבטחת המידע למסור בפני ועדת היגוי לנושאי אבטחת מידע, דיווח מפורט על ביקורת ביצוע של נוהל זה.

## 10. הוראות עבודה נגזרות

- 10.1. טיפול ברשומות ארגוניות לצורך ארכוב וגניזה
- 10.2. תפעול כרטיסי אשראי על פי תקן PCI DSS

### לשימוש פנימי בלבד

זכויות יוצרים "מאחדת" © - מסמך זה והידע הכלול בו הינו קניינה הבלעדי של מאחדת ואסור לשימוש ו/או לפרסום ו/או לגילוי ו/או להפצה ו/או להעתקה ו/או בחלקו, במישרין, ו/או בעקיפין ללא הסכמה מראש ובכתב של מאחדת.