

<b>חל"י – חברה ממשלתית להגנות ים-המלח בע"מ</b>	
שם הנוהל:	טיפול במאגרי מידע המחוייבים ברישום
פרק:	תפעול ומינהל
פרק משנה:	
אישור הנוהל:	
מס' נוהל:	מס' נוהל מס':
בתוקף מיום: 2019	מבטל נוהל מס':
	מיום:
	עמוד 1 מתוך 8

## 1. כללי

הזכות לפרטיות היא מהחשובות שבזכויות האדם בישראל. חוק הגנת הפרטיות, התשמ"א - (1981 להלן: "חוק הגנת הפרטיות" או "החוק") והתקנות שהותקנו מכוחו (להלן: "התקנות") באים להגן על זכויות הפרט ולעגן אותן בחוק מפורש. בהתאם לחוק, פגיעה בפרטיותו של אדם היא עוולה על פי דיני הנזיקין ואף במקרים מסוימים עבירה פלילית. החברה הממשלתית להגנות ים המלח בע"מ (להלן: "חל"י" או "החברה") עושה כל שביכולתו על מנת לקיים אחר דרישות החוק והתקנות לרבות בדבר החזקת מאגרי מידע.

## 2. מטרות

- 2.1. הגדרת כללי אבטחת המידע המחייבים את החברה, עובדיה וספקיה.
- 2.2. התאמת פעילות החברה להוראות החוק, לתקנות שהותקנו מכוחו ובפרט לתקנות הגנת הפרטיות ואבטחת המידע ולהנחיות הרשות להגנת הפרטיות, כפי שיעודכנו מעת לעת.
- 2.3. מימוש תכליות החוק והגנה על זכויות נושאי המידע במאגרי המידע מפני שימוש לרעה במידע אודותיהם, הן ע"י גורמים מחוץ לחברה והן ע"י העובדים.
- 2.4. הגדרת פעולות ובקורות הנדרשות לעמידה בדרישות החוק ותקנות הגנת הפרטיות ואבטחת המידע.

## 3. הגדרות

- 3.1. שימוש במאגר מידע – שימוש במידע כגון: עיבוד, שינוי, עדכון, העתקה וצפייה בו.
- 3.2. משתמש – כל מי שעושה שימוש במידע המצוי במאגר מידע ממוחשב
- 3.3. בעל הרשאה – כהגדרתו בתקנה 1 לתקנות אבטחת מידע.
- 3.4. מידע רגיש – כהגדרתו בחוק הגנת הפרטיות (כפי שתהא מעת לעת), ובאופן כללי: נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו.
- 3.5. מאגר המידע – אוסף נתוני המידע, המוחזק באמצעי מגנטי ו/או אופטי ו/או ממוחשב מכל סוג שהוא והמיועד לעיבוד ממוחשב, למעט אוסף לשימוש אישי שאינו למטרות עסק ולמעט אוסף הכולל רק שם, מען ודרכי התקשרות, ובלבד שאין אוסף נוסף ובו פרטים נוספים לגבי אנשים אלה הנכללים באוסף.
- 3.6. אבטחת מידע – הגנה על שלמות המידע או הגנה על המידע מפני חשיפה, שימוש או העתקה ללא רשות.
- 3.7. בעל מאגר מידע – בעל מאגרי המידע הוא חל"י.
- 3.8. מנהל מאגר המידע – מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה. מנהל המאגר מוביל ומנהל את מערכת ההגנה על המידע במאגרים.
- 3.9. מחזיק מאגר – ספק שמנהל/מחזיק מערכת למאגר מידע דרך קבע והוא רשאי לעשות בו שימוש.
- 3.10. אחראי המיחשוב – עובד החברה או נותן שירותים האמון על יישום טכנולוגיה בחברה.
- 3.11. נושאי מידע במאגר – בני האדם ששמותיהם ופרטיהם כלולים ומופעים במאגר (עובדים, לקוחות, מועמדים, או כל אדם אשר פרטיו מופעים במאגר).

<b>חל"י – חברה ממשלתית להגנות ים-המלח בע"מ</b>	
שם הנוהל:	טיפול במאגרי מידע המחוייבים ברישום
פרק:	תפעול ומינהל
פרק משנה:	מבטל נוהל מס':
אישור הנוהל:	מיום:
	עמוד 2 מתוך 8

#### 4. תחום ומידע ארגוני

- 4.1. מדיניות אבטחת מידע זו וכל הנהלים וההנחיות הנגזרים ממנה חלים על כלל עובדי החברה בכל רמה היררכית שהיא לרבות עובדי צד ג' העובדים מטעמה או נותני שירותים.
- 4.2. מערך המיחשוב של החברה מאוחסן ושומר במתחם החברה וחלקו בשירות ענן (SAAS), כאשר הגישה אליו ולמידע האגור בו ומעובד על ידו אפשרית ומותרת בהתאם לתפקיד וההרשאה שהוקצתה לבעל תפקיד על ידי מנהל המאגר.
- 4.3. השימוש במאגר המידע יהיה בהתאם למטרה להם נועד המידע ולשמו נאסף ונאגר.

#### 5. סמכות ואחריות

- 5.1. באחריות מנהל מאגר מידע:
- מנהל מאגר מידע אחראי על קביעת מדיניות אבטחת מידע על מנת להבטיח קיום הוראות החוק והתקנות בתחומים הבאים:
- 5.1.1. רישום של המאגר אצל הרשם
- 5.1.2. דיווח על שינויים בפרטי המאגר
- 5.1.3. מתן אפשרות לפרט לעיון במידע אודותיו ותיקונו במידה והמידע אינו נכון/מעודכן, למעט במקרים המצויינים בחוק (כגון חסיון כלשהו, מידע רפואי)
- 5.1.4. אבטחת המידע. תוך שימת לב לנושאים הבאים:
- 5.1.4.1. הגנה פיזית על מידע
- 5.1.4.2. מדיניות הגישה למידע
- 5.1.4.3. אישור או מניעת העברת וחשיפת מידע לגורם חוץ
- 5.1.4.4. בקורות תקופתיות
- 5.1.4.5. מדיניות הגיבויים ושמירה של מידע
- 5.1.4.6. הגברת המודעות לאבטחת מידע בחברה
- 5.1.5. פיקוח ובקרה על יישום מדיניות אבטחת מידע.
- 5.1.6. החברה נותנת מנהל המאגר את מלוא הגיבוי והאפשרויות למלא את המוטל עליו, ומקצה לשם כך את המשאבים הנדרשים לכך.
- 5.1.7. באחריות מנהל המאגר להכין וליישם תכנית בקרה שוטפת על עמידת החברה בדרישות הנגזרות בתקנות, בחוק ונוהלי אבטחת המידע שהנהלה אימצה.
- 5.1.8. מנהל המאגר יודא תקיפות ועדכניות מסמך זה וכלל הנהלים הנגזרים מהתקנה ומסמך זה.
- 5.1.9. אחראי המיחשוב יפעל מטעם מנהל מאגר המידע בתחומים אשר נדרשת מיומנות מיקצועית, בתחומי מיחשוב בכלל ואבטחת מידע בפרט
- 5.2. באחריות אחראי המחשוב:

<b>חל"י – חברה ממשלתית להגנות ים-המלח בע"מ</b>	
שם הנוהל:	<b>טיפול במאגרי מידע המחוייבים ברישום</b>
פרק:	תפעול ומינהל
פרק משנה:	מס' נוהל: 2019
אישור הנוהל:	מבטל נוהל מס': מיום: עמוד 3 מתוך 8

באחריות האחראי לתחזק את מאגר המידע בהתאם לדרישות של בעל המאגר ומנהל המאגר, ובכלל זה להבטיח כי:

- 5.2.1. המערכות שמאחסנות את המידע נמצאות במקום ייעודי מוגן עם תשתית מיזוג אוויר וכיבוי אש מתאימים.
- 5.2.2. הגישה הפיזית למערכות מוגבלת למורשים בלבד. כל גורם מקצועי לא מורשה יקבל ליווי בעת ביצוע העבודות.
- 5.2.3. להגדיר את המערכת ולתחזק אותה בהתאם למדיניות וסדרי הניהול אשר ייקבעו בשיתוף עם בעל מאגר המידע.
- 5.2.4. לבצע גיבוי למידע בהתאם למדיניות הנקבעת בשיתוף בעל מאגר המידע. על מחזיק המאגר לבצע בדיקה תקופתית של הגיבויים ע"י שחזורים יזומים כדי לוודא שהמידע אמין וניתן לשחזור בעת הצורך.
- 5.2.5. לנקוט אמצעי אבטחה סבירים כגון, חומת אש, IPS, IDS, אנטיירוס ועוד, בהתאם לרמת רגישות המידע, שימנעו חדירה מכוונת או מקרית למערכת.

## **6. רישום והעברת מידע**

### **6.1. רישום מאגרי המידע**

- 6.1.1. מנהל המאגר בחברה ירשום את המאגר כחוק וינחה את מנהל המאגר ומתפעל המאגר בכל הנדרש והנוגע לדרכי הטיפול במידע, איסופו ואבטחתו כנדרש על פי החוק ועל פי מדיניות החברה.
- 6.2. העברת מידע ממאגר מידע רשום בין החברה לבין גופים אחרים  
העברה ו/או חשיפת מידע לגופים מחוץ לחברה לא תיעשה אלא באישור מנהל המאגר.
- 6.3. סודיות  
לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמשתמש, כמנהל או כמתפעל מאגר מידע אלא לצורך ביצוע עבודתו או לביצוע הוראות החוק.

## **7. ניהול נכסים וסיכונים**

- 7.1. באחריות מנהל המאגר לקיים הליך של ניהול נכסים וסיכונים על נכסי המידע בחברה, ועל מאגרי המידע.
- 7.2. הנהלת החברה זיהתה ומיפתה את מאגרי המידע שברשותה תוך פירוט הנקודות הבאות:
  - 7.2.1. פרטי מאגר המידע.
  - 7.2.2. מטרת האיסוף והשימוש במידע.
  - 7.2.3. פרטים הנוגעים לשימוש במידע מחוץ לגבולות המדינה – לא רלוונטי. אין שיתוף של מאגרי מידע פרטיים לגורמים מחוץ לגבולות המדינה.
  - 7.2.4. פרטי מנהל מאגר המידע.
  - 7.2.5. פרטים הנוגעים לסיכוני אבטחת המידע ואופן ההתמודדות עמם.
- 7.3. ראה קובץ מצורף "מיפוי מערכות מידע" רשימת מאגרים.
- 7.4. באחריות מנהל מאגר המידע בחברה לתקף מסמך מיפוי נכסי החברה מידי תקופה אך לפחות פעם בשנה.

## **8. אבטחה פיזית וסביבתית**

<b>חל"י – חברה ממשלתית להגנות ים-המלח בע"מ</b>	
שם הנוהל:	טיפול במאגרי מידע המחוייבים ברישום
פרק:	תפעול ומינהל
פרק משנה:	מבטל נוהל מס' :
אישור הנוהל:	מיום :
	עמוד 4 מתוך 8

- 8.1. משרדי החברה שוכנים במתחם מוגן ומנוטר באמצעים פיזיים ואלקטרוניים.
- 8.2. מתחם המשרדים מנוטר באמצעות מצלמות מעקב גלויות, המתריעות ומתעדות תנועה.
- 8.3. מערכות המידע והתקשורת אשר מאחסנות ומעבדות את המידע הארגוני נמצאות בחדר שרתים נעול וממודר וחלקן בענן בשירות SAAS.
- 8.4. באחריות אתראי המחשוב לתעד כל הכנסת או הוצאת תשתיות ומערכות מידע בכלל והנוגעות למאגרי המידע בפרט.
- 8.5. באחריות מנהל המאגר לוודא כי מצעי מידע המכילים מידע בכלל ומאגר מידע בפרט אשר יצאו מכלל שימוש, יושמדו באמצעי פיזי.
- 8.5.1. כונני מחשב ו/או כל מצע מידע נייד יגרסו או יעשה בהם נזק משמעותי (קידוח).
- 9. ניהול אבטחת משאבי אנוש**
- 9.1. עובדי החברה, במסגרת עבודתם, חשופים למידע רב הכולל מידע רגיש מהיבטים עסקיים ואישיים של החברה ושל הלקוחות, לאור זאת תינתן תשומת לב רבה לאמינות העובד, יושרו וכישוריו בכל תקופת עבודתו בחברה.
- 9.2. נציגי ההנהלה יבטיחו כי העובדים בחברה לרבות גורמי צד ג' מתאימים לתפקיד שיועד להם, מבינים את האחריות המוטלת עליהם לשם מניעת מקרי כשל, הונאה או שימוש לרעה במידע ונכסי החברה והלקוחות.
- 9.3. מהימנותם של עובדי החברה תיבדק לפני קליטתם באמצעות תשאול ממליצים ו/או באמצעות בחינה של גורם חיצוני, בהתאם לצורך התפקודי ומידת חשיפתם למידע רגיש.
- 9.4. כל עובד, בכל רמה היררכית שהיא, יחתום על הסכם שמירת סודיות וחיסיון NDA כתנאי לעבודתו בחברה.
- 9.5. לפני התחלת העבודה יעבור העובד החדש הדרכה להכרת החברה ונוהלי אבטחת המידע בפרט. לפחות פעם בשנה יעברו כלל עובדי החברה הדרכה להעלאת המודעות להיבטי אבטחת מידע בכלל ואבטחת מידע אישי רגיש בפרט.
- 9.6. הקצאת הרשאות גישה למערכות המחשב של החברה תתבצע רק עם תום תהליך הקליטה וחתירת העובד על הסכמי הסודיות הנדרשים.
- 9.7. בעת מעבר מתפקיד לתפקיד באחריות הצוות הניהולי של החברה לוודא כי מהימנותו ואמינותו של העובד אכן מתאימים לתפקיד החדש, תוך מתן דגש לחשיפה למידע אישי רגיש. יש לתת את הדעת להרשאות ולבקורות הגישה אשר היו לעובד בתפקיד הקודם מול ההרשאות החדשות המוקצות לו. כברירת מחדל, יחסמו ההרשאות של התפקיד הישן, ותפתחנה לעובד הרשאות חדשות התואמות את התפקיד החדש.
- 9.8. עם עזיבת עובד את החברה, מכל סיבה שהיא, על הממונה הישיר לקיים הליך מסודר ובטוח ובהתאם לחוק, ולהבטיח כי העובד החזיר את נכסי החברה אשר ברשותו, והרשאותיו במערכות המידע נחסמו.
- 9.9. באישור נציג הנהלה, ניתן יהיה להעביר תוכן תיבת דואר אלקטרוני של עובד שעזב לעובד אחר.
- 10. ניהול הרשאות גישה**
- 10.1. הנהלת החברה קבעה את הכללים הבאים כמדיניות הקצאת הרשאות גישה:
- 10.1.1. הצורך לדעת בלבד – Need to Know.

<b>חל"י – חברה ממשלתית להגנות ים-המלח בע"מ</b>	
שם הנוהל:	טיפול במאגרי מידע המחוייבים ברישום
פרק:	תפעול ומינהל
פרק משנה:	מבטל נוהל מס':
אישור הנוהל:	מיום:
	עמוד 5 מתוך 8

10.1.2. הפרדת תפקידי מפתח - Segregation of Duties

10.1.3. פיצול סמכויות (תפעול, בקרה ואישור).

10.1.4. הימנעות מהרשאות יתר ורחבות.

10.1.5. הקצאת הרשאות למשתמשי המערכת תתבצע בהתאם לתפקיד המוגדר ובאישור בעל המידע.

10.1.6. לא יהיה שימוש בשמות משתמש ציבוריים על ידי מספר משתמשים.

10.2. ניהול גישת משתמשים:

10.2.1. הקצאת קוד משתמש למערכות הממוחשב של החברה תהייה רק לאחר שהעובד סיים את תהליך הקליטה וחתם על הסכם הסודיות.

10.2.2. מנהל מאגר המידע בחברה יחד עם נציגי ההנהלה השונים (בעלי המידע) יגדירו מבנה הרשאה בחתך תפקיד, תוך מתן תשומת לב למדיניות הקצאת ההרשאות ולמידת רגישות המידע אשר תיחשף לבעל התפקיד.

10.2.3. באחריות הממונה הישיר של העובד לבקש את ההרשאות המגיעות לעובד בהתאם לתפקיד.

10.2.4. הוגדר תהליך מובנה להקמת משתמש במערכת, הכולל עדכון תכולת ההרשאה וחסימתה עם עזיבת עובד את החברה ו/או מעבר לתפקיד אחר.

10.2.5. הקצאת הרשאות רחבות למשתמשי המערכת תיעשה באישור בעלי המידע תוך קביעת בקרות בעת ביצוע פעולות במידע או תהליך רגיש.

10.2.6. במסגרת מיפוי וזיהוי מאגרי המידע וסקר הערכת סיכונים בתהליך יזוהו בעלי התפקיד והעובדים אשר יש להם גישה למאגרי המידע הרגישים בארגון.

10.2.7. לפחות פעם בשנה, יתקיים סקר משתמשים במערכות הארגון, לוודא כי רק במערכת פתוחים רק משתמשים אשר עובדים בחברה, ועובדים אשר עזבו נחסמו, באחריות מנהל מאגר המידע.

## 11. זיהוי ואימות

11.1. לכל משתמש מערכות המידע בחברה הוגדר קוד משתמש וסיסמא חד-חד ערכית (User ID & Password) אישיים אשר ידועים רק לו.

11.2. סיסמת הגישה למערכות המידע בכלל ולמאגרי מידע רגיש בפרט, תהייה מוקשחת בהתאם לנדרש בתקנה 9 לחוק.

11.3. חל איסור מוחלט למסור לכל גורם שהוא את הסיסמא, למניעת שימוש לרעה.

11.4. בהתאם לנדרש בתקנה 9 לחוק, כל פעילות המתבצעת במערכות ומאגרי מידע רגישים מתועדת במערכת הלוגים תוך קיום הליך של זיהוי ועקיבה אחר מבצע הפעולה.

11.5. מדיניות סיסמאות: ראה מסמך "מדיניות אבטחת מידע במערכת המחשוב של החברה"

## 12. בקרה ותיעוד גישה

12.1. גישת משתמשים לטבלאות המערכת בכלל ולמאגרי מידע רגיש פרט מתועדת במערכות הלוגים של מערך המחשוב.

<b>חל"י – חברה ממשלתית להגנות ים-המלח בע"מ</b>	
שם הנוהל:	<b>טיפול במאגרי מידע המחוייבים ברישום</b>
פרק:	תפעול ומינהל
פרק משנה:	מס' נוהל:
אישור הנוהל:	בתוקף מיום: 2019
	מבטל נוהל מס':
	מיום:
	עמוד 6 מתוך 8

12.2. עם קרות אירוע חריג במערכת התפעולית, ניתן לקיים הליך של בקרת זהות המשתמש לצורך תחקור והפקת לקחים.

### **13. אירוע אבטחת מידע**

13.1. הגדרה מתוך התקנה - אירוע אבטחה חמור" - כל אחד מאלה:

13.1.1. במאגר מידע שחלה עליו רמת אבטחה בינונית - אירוע שנעשה בו שימוש בחלק מהותי מן המאגר בלא

הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע לגבי חלק מהותי מן המאגר;

13.2. הוגדר תהליך אשר יבטיח טיפול מהיר באירוע תוך נקיטת פעילות מתקנת למזעור הסיכון וכל נזק אפשרי, וכן קיום הליך של הפקת לקחים למניעת הישנות המקרה.

13.3. על עובדי החברה, בכל רמה היררכית שהיא לרבות עובדי צד ג' לדווח לממונים עליהם ו/או לאחראי המחשוב על כל נקודת כשל אפשרית בהיבט אבטחת מידע או על כל אירוע או חשד לאירוע אבטחתי למניעת החרפת המצב.

13.4. משתמשי המערכת לא יטפלו או לא יבצעו כל פעילות תיקון או מנע ללא הנחיית מנהל המאגר או מי מטעמו.

13.5. בעת קרות אירוע חריג בהיבט אבטחת מידע או חשד, יערך הליך מזעור הנזק, תחקיר והפקת לקחים לשם לימוד ומניעה בעתיד.

13.6. הנהלת החברה מינתה את מנהל מאגר המידע כאחראי לטיפול באירוע חריג, תוך מתן פתרון הולם ואפקטיבי לחזרה מהירה לשגרה ומזעור נזקים אפשריים.

13.7. מהלך הטיפול באירוע יתועד ויתוחקר לשם הפקת לקחים למניעת הישנות המקרה.

13.8. במידה והאירוע נבע מחריגה ממדיניות אבטחת המידע והנהלים הנגזרים ממנה, יתקיים בירור והליך משמעותי עם העובד ע"י הממונה הישיר ו/או נציג ההנהלה.

13.9. בתום הטיפול באירוע, ייערך "תחקיר אירוע" ובו תיאור המקרה, תמצית הממצאים, דרך הטיפול בהם ומסקנות. התחקיר יופץ להנהלת החברה, וישמש כבסיס להערכת נזקים, הפקת לקחים, אימוץ פתרונות אבטחתיים מתאימים. לפחות פעם בשנה תתקיים ישיבת הנהלה בנושאי אבטחת מידע בכלל ו"אירוע חריג" בפרט.

13.10. בהתאם לתקנה 11 אשר חוק הגנת הפרטיות, התשמ"א-1981, על מנהל מאגר המידע בחברה חלה החובה לדווח לרשם במשרד המשפטים עם קרות אירוע אבטחה חמור, הדבר ייעשה בתיאום עם מנכ"ל החברה באופן מידי עם קרות האירוע.

13.11. הדיווח לרשויות הממלכתיות יכלול תיאור האירוע, צעדים שננקטו עד עתה, וכן דיווח שוטף עד החזרה לשגרה.

13.12. מומלץ לידע ולהתייעץ עם הרשות הלאומית להגנת הסייבר לשם קבלת כלים נוספים לטיפול באירוע.

13.13. לפי מידת חומרת האירוע ו/או הנחיית הגורם הממלכתי, על בעל המידע / מנכ"ל החברה להודיע לנשואי המידע בדבר האירוע וההשלכות לגבי מאגר המידע.

### **14. התקנים ניידים ועבודה מרחוק**

<b>חל"י – חברה ממשלתית להגנות ים-המלח בע"מ</b>	
שם הנוהל:	טיפול במאגרי מידע המחוייבים ברישום
פרק:	תפעול ומינהל
פרק משנה:	מבטל נוהל מס':
אישור הנוהל:	מיום:
	עמוד 7 מתוך 8

14.1. עובדי החברה, בכל ההירכיה שהיא מתבקשים להימנע משימוש במצעי מידע ניידים Disk On Key או אחרים, לכל מטרה שהיא.

14.2. השימוש במחשב נייד אפשרי ומותר לשימוש לעובדי החברה לצורך מילוי תפקידם בחברה במתחם החברה ומחוצה לה, תוך שימוש בבקורות וההגנות אשר הותקנו ע"י אחראי המחשוב.

14.3. לפי מידת הצורך התפקודי תתאפשר למשתמשי מערכות המידע התחברות מרחוק למערכות המיחשוב של החברה תוך שימוש בבקורות ובהגנות יעודיות לדבר (VPN SSL).

14.4. לפחות פעם בשנה יתבצע סקר משתמשים המתחברים מרחוק אשר יאושר ע"י הנהלה החברה.

14.5. חל איסור מוחלט למשתמש לאגור מידע מסווג (רגיש) במצעי מידע ניידים ונתיקים.

#### **15. ניהול מאובטח ומעודכן של מערכות המאגר**

15.1. לשם אבטחה נאותה על מאגרי המידע אשר מאוחסנים ומעובדים במערכות המחשב והתקשורת מתקיים הליך ניטור ובקרה אוטומטי אשר שולח הודעות שוטפות לאחראי המחשוב בדבר תקינות או אי תקינות התהליך.

15.2. אחראי המחשוב מקבל דיווח שוטף בדבר תקינות ונאותות הבקורות ותהליכי העבודה הממוחשבים בחברה.

15.3. במערכות המידע של החברה מותקנות בקורות והגנות ייעודיות לשם קיום אבטחת מידע כולל על המערכות בכלל ועל המידע בפרט.

15.4. הגישה למערכות תפעוליות אשר מעבדות מידע רגיש תהייה ממודרת, כאשר הגישה למערכת ולמידע אשר בה למשתמשים מורשים בלבד.

#### **16. אבטחת תקשורת**

16.1. לצורך עמידה בדרישות אבטחת מידע (חיסיון, זמינות ושלמות) מתוקנות בקורות והגנות ייעודיות ברשת המחשבים של החברה, כאשר כל הניהול, המערכות ומאגרי המידע נמצאים במקום ריכוזי אחד.

**ראה מסמך "מדיניות אבטחת מידע במערכת המחשוב של החברה"**

#### **17. מיקור חוץ**

17.1. מערכות המידע והתקשורת של החברה מתוחזקות על ידי אחראי המחשוב, לפי מידת הצורך והעניין, כאשר נדרש ידע של מומחה ו/או תיגבור, יועסק גורם צד ג' לנושא לאחר שחתם על הסכם סודיות.

17.2. לפי מידת הצורך והעניין ולצורכי עבודה בלבד, ניתנת גישה לגורם צד ג' לתחוק ולטפל במערכות המידע של החברה מרחוק, אך הדבר נעשה לפי בקשה מיוחדת ובאישור מנהל מאגר המידע, תוך שימוש בקווי תקשורת מוגנות ומאובטחות (VPN SSL).

<b>חל"י – חברה ממשלתית להגנות ים-המלח בע"מ</b>	
שם הנוהל:	<b>טיפול במאגרי מידע המחוייבים ברישום</b>
פרק:	תפעול ומינהל
פרק משנה:	מבטל נוהל מס':
אישור הנוהל:	מיום:
	עמוד 8 מתוך 8

17.3. אחריות מנהל המאגר בארגון, לקיים סקר בעלי הרשאות גישה מרחוק ע"י גורמי צד ג', ולאשרם ע"י נציג הנהלה, ולתקף את הסכמי הסודיות.

*ראה מסמך "מדיניות אבטחת מידע במערכת המחשוב של החברה"*

#### **18. גיבוי ושחזור**

18.1. באחריות משתמשי מערכות המידע לשמור את המידע וכל פעילות מחשב שהיא ברשת הארגונית ולא בכוננים האישיים אשר אינם מגובים.

18.2. מידי יום, מתבצע גיבוי המידע האגור והמעובד במערכות המידע של החברה באמצעות תוכנה ייעודית המופעלת אוטומטית. ראה מסמך " מדיניות מידע במערכת המחשוב של החברה"

18.3. מערכת ניטור ובקרה אוטומטית מבקרת ומנטרת את פעילות הגיבוי האוטומטי, במידה ומזוהה תקלה או פעילות לא סדירה בתהליך הגיבוי, נשלח מייל לאחראי המחשוב

18.4. לפי מידת הצורך יטפל אחראי המחשוב בתקלה לפי הנחיות מערכת הגיבוי.

18.5. הגיבוי השבועי נשמר במקום מוגן בכספת החברה.

18.6. לפחות פעם בשנה באחריות מנהל המאגר לקיים שיחזור מדגמי לשם בקרת תקינות תהליך הגיבוי.

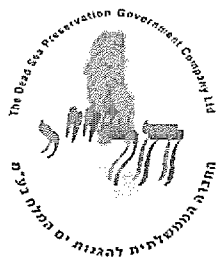
#### **19. ביקורות תקופתיות**

19.1. לפחות פעם בשנה יערך מבדק פנימי במערכת ניהול אבטחת המידע בחברה.

19.2. במבדק הפנימי תבחן מידת עמידת החברה ביישום נוהל אבטחת מידע זה וההנחיות הנגזרות ממנו, וכן עמידת החברה בתקנות הגנת הפרטיות אבטחת מידע התשע"ז-2017.

19.3. המבדק הפנימי יתבצע על ידי גורם חיצוני לארגון או אשר אינו נושא הביקורת (אינו נמנה בין אחראי המחשוב).





לכבוד  
החברה הממשלתית להגנות ים המלח  
ירושלים

### הצהרת סודיות

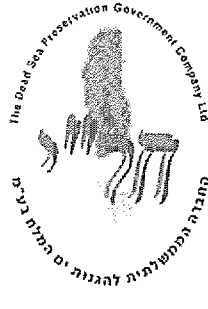
הריני, \_\_\_\_\_ ת.ז. מס' \_\_\_\_\_ מצהיר ומאשר בזאת כדלקמן:

- ידוע לי כי במהלך עבודתי בחברה הנני נחשף לחומר ומידע (בגין בנייר ובין בקבצי מחשב וכיוצ"ב), שהינו מידע סודי ורגיש של החברה. בכלל זאת, מידע כולל מסמכים, דוחות, טבלאות, תוצאות של הליכים מכרזיים ותחרותיים, אומדנים, ניתוח מחיר, ניתוחי מידע, הגשות של קבצים ומסמכים על ידי צדדים שלישיים לרבות במסגרת מכרזים והליכים תחרותיים מכל סוג שהוא, דברים שנאמרים בעל פה (לרבות במסגרת ישיבות ופגישות), וכיוצ"ב.
- ידוע לי כי חומר ומידע כאמור לעיל, מכל סוג ובכל פורמט שהוא (להלן: "המידע"), המגיעים אלי תוך כדי עבודתי בחברה (בין אם הועברו אלי ע"י החברה ובין אם ע"י צדדים שלישיים), כולל סודות רגישים אשר גילויים עלול לגרום לחברה ו/או לקוחותיה ו/או נותני השירותים מטעמה ו/או לצדדים שלישיים, נזקים חמורים.
- אני מתחייב בזה שלא לגלות ו/או להעביר במישרין ו/או בעקיפין את המידע לכל אדם ו/או גוף, לרבות עובדי החברה ו/או נותני השירותים מטעמה ו/או כל צד שלישי, בין במישרין ובין בעקיפין, ללא אישור הממונה עלי, וכן לא להורות לעובד אחר לעשות כן אלא אם הדבר במפורש בסמכותי.
- אני מתחייב לשמור באופן זהיר ודקדקני את המידע, באופן שלא יאפשר גישה ו/או עיון ו/או העתקה של המידע על ידי כל צד שלישי שהוא, לרבות עובדים אחרים בחברה שאינם מורשים לכך במפורש ובכתב.
- ידוע לי שאם אפר אחת או יותר מהתחייבויותי דלעיל, אני עובר עבירה משמעתית חמורה.
- התחייבויותי דלעיל תהיינה תקפות ללא הגבלה בזמן גם אם אפסיק את עבודתי בחברה מכל סיבה שהיא.

על כך באתי על החתום:

\_\_\_\_\_ חתימה:

\_\_\_\_\_ תאריך:

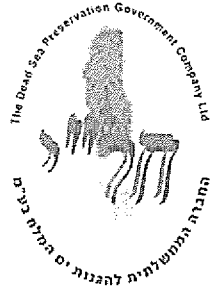


## חוזר אבטחת מידע לעובד

1. **מטרת החוזר**

להביא לידיעת עובדי החברה את מדיניות החברה ביחס לאופן השימוש הנאות והנכון במערכות המידע והמחשוב של החברה במטרה להגן על חיסיון, זמינות ושלמות המידע הארגוני ומניעת הגעתו לידי גורם שלא הוסמך לכך, תוך מתן דגש והבהרת האחריות החלה על כל משתמש בשמירה על כללי אבטחת המידע והפרטיות.
2. **מידע וציוד מחשוב**
  - א. שמירת מידע - תעשה בכונני הרשת בלבד. על אף האמור לעיל, במהלך עבודה עם מחשב נייד במקום בו אין גישה לכונן רשת, ניתן לשמור באופן זמני מידע בכונן המקומי ולהעבירו מיד כשהדבר ניתן לכונן הרשת הרלוונטי. כל מידע שישמר שלא בכונן הרשת לא מוגן ולא מגובה ולכן לא יהיה ניתן לבצע שיתזור של המידע שאבד ו/או ניזוק.
  - ב. הוצאת מידע - תיעשה אך ורק לצרכי עבודה.
  - ג. הכנסת ציוד מחשוב לחברה והוצאתו אסורה ללא אישור סמנכ"ל תפעול ומינהל. ההוראה אינה חלה על ציוד נייד מעצם טיבו, כגון: מחשבים ניידים.
  - ד. עובדים נדרשים להשתמש רק בדיסק און קי שהוצפן על ידי ספק שרותי המחשוב.
3. **סיסמא**
  - א. סיסמא ושם משתמש הם אישיים ואין לתת לאחרים זכות להשתמש בהם. אין להשתמש בשם משתמש ו/או בסיסמא קבוצתיים, אין למסור את הסיסמא לאדם ו/או גורם אחר.
  - ב. החלפת הסיסמא ותדירות החלפתה תיעשה עפ"י כללים פרטניים לסוגיה זו.
  - ג. אין לרשום את הסיסמא במקום נגיש וחשוף ואין להשתמש בתכנה ו/או בהליכי זיהוי אוטומטיים המאפשרים עקיפה של הקשת שם המשתמש והסיסמא באופן ידני.
4. **אינטרנט**
  - א. השימוש באינטרנט ובשירותים הנלווים יבוצעו לצורכי ומטרות עבודה.
  - ב. הגלישה והשימוש באתרי סקס/ פורנוגרפיה, הימורים, אתרי הסתה, גזענות – אסורים בהחלט.
5. **חשבון דואר אלקטרוני ארגוני**
  - א. הדואר האלקטרוני הנו כלי עבודה, השימוש בו מותר לצורכי ומטרות עבודה.
  - ב. אין לבצע הפניה קבועה של דואר אלקטרוני המתקבל לחשבונכם הארגוני אל

### חשבון דואר אחר



ג. כל עובד בעל גישה למערכת הדוא"ל של החברה ממכשיר הטלפון הנייד שלו מחויב בהגדרת סיסמה מספרית (לא תבנית צורנית) ו/או טביעת אצבע לצורך גישה למידע שבמכשירו.

**6. חיסיון בשמירה על צנעת הפרט והעברת מידע הנוגע לענייני החברה**

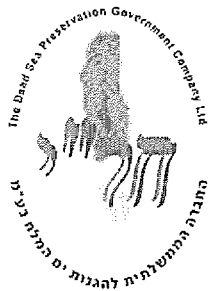
- א. העברת מידע הנוגע לצנעת הפרט של עובד בחברה לכל גורם, שלא לצרכי עבודה, אסורה בהחלט. על הגורם המעביר לוודא, כי הגורם הנעבר אכן זכאי ורשאי לקבל את המידע המבוקש ובמקרה של ספק להתייעץ עם הממונה עליו.
- ב. על כל עובד בחברה, חל איסור על העברת מידע הנוגע לענייני החברה שלא לצרכי עבודה, אסורה בהחלט. על הגורם המעביר לוודא, כי הגורם הנעבר אכן זכאי ורשאי לקבל את המידע המבוקש ובמקרה של ספק להתייעץ עם הממונה עליו.
- ג. לעניין העברת מידע שאושרה העברתו, יש להקפיד על חיסיון בשמירה על צנעת הפרט בתכנים ומסרים המועברים באמצעות הדואר האלקטרוני, בעת השימוש באינטרנט, ובכל אמצעי או דרך של העברת מידע.

**7. התקנה, תחזוקה שוטפת ושדרוג**

- א. התקנה, תחזוקה שוטפת ושדרוג של ציוד מחשוב (Pc, מחשב נייד, שרתים וכו') מדפסות, מודמים, מערכת מידע (חומרה - Hardware, או תכנה - Software) תבוצע אך ורק ע"י הספקים היעודיים של החברה למטרות אלו.
- ב. אין לשכפל, להעתיק ולהפיץ תוכנות ורישיונות ארגוניים וכן נתונים או מידע מכל סוג לשימוש מחוץ לחברה, לשימוש פרטי או לכול מטרה אחרת מכל סוג אחר.
- ג. אין להתקין ולחבר רכיב תוכנה או חומרה או קבצי מידע – לשימוש פרטי במערכות המידע והמחשוב של החברה.
- ד. התקנה או חיבור בכל דרך שהיא של רכיב תכנה או חומרה או קבצי מידע – לצרכי עבודה במערכות המידע והמחשוב של החברה מחייבת קבלת אישור מראש על ידי סמנכ"ל תפעול ומינהל. הוראה זו אינה חלה על שימוש בהתקן נתיק לצורך אישור ביצוע תשלומים במערכת המס"ב.

**8. מדיניות מסך נקי (Clear Screen Policy)**

ככלל מסך המחשב בכל עמדת עבודה ינעל אוטומטית לאחר פרק זמן מוגדר, בו לא יעשה שימוש בעמדת המחשב. יחד עם זאת, על כל משתמש לנעול את המסך באופן יזום כל אימת שהדבר נחוץ על מנת למנוע סיכון לחשיפת מידע אסורה.



**9. מדיניות שולחן נקי ( Clear Desk Policy )**

יש לדאוג שמסמכים, דוחות ומידע ממוחשב מסווג ישמרו באופן נאות על מנת למנוע את חשיפתם לגורמים לא מורשים. לפיכך ביחס למסמכים רלוונטיים ינקטו הצעדים הבאים: יאוחסנו במקום סגור ומאובטח; ישונעו בתיק ו/או מעטפה סגורים; יגרסו בעת הצורך.

**10. מדיניות בקרה**

החברה שומרת לעצמה את הזכות לבדוק/לפקח על קיום המדיניות המפורטת בחוזר זה בכל אמצעי מקובל, חוקי ונדרש בהתאם לנסיבות העניין. החברה תעשה כל מאמץ לשמור על פרטיות המשתמש.

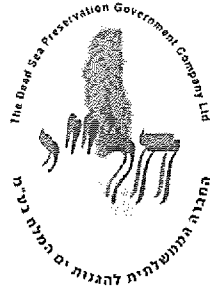
**11. הגנת מסמך**

ניתן להגן על מסמכים (אקסל, וורד, וסוגי מסמכים נוספים), מפני פתיחה ו/או צפייה ע"י גורמים לא מורשים, באמצעות שמירת המסמך בצרוף סיסמא. שיטה זו מומלצת בהעברת מידע רגיש באמצעות דואר אלקטרוני וכו'.  
הערה: אין לכלול את הסיסמא איתה שמרתם את המסמך בגוף הודעת הדואר האלקטרוני המכילה את המסמך עצמו.  
לתשומת לב: מסמך שנשמר עם סיסמא לפתיחה / קריאה, לא תתאפשר פתיחת המסמך במידה והסיסמא אבדה ו/או אינה זכורה לכם, לא ניתן יהיה לשחזרו/להצילו.

**12. דיווח על אירועי אבטחת מידע**

כל אירוע אבטחת מידע המתגלה לעובד, יש להעביר את פרטיו מיידית לסמנכ"ל תפעול ומינהל.

**THE DEAD SEA PRESERVATION  
GOVERNMENT COMPANY LTD**



**החברה הממשלתית  
להגנות ים המלח בע"מ**

## **חוזר אבטחת מידע**

### הצהרת משתמש

1. פרטי המשתמש

שם פרטי: \_\_\_\_\_ שם משפחה: \_\_\_\_\_

2. אישור המשתמש

הנני מצהיר/ה כי קראתי והבנתי את חוזר "אבטחת מידע" והנני מתחייב/ת לנהוג עפ"י  
הנחיותיו

חתימה: \_\_\_\_\_ תאריך: \_\_\_\_\_