שם הנוהל: מדיניות אבטחת מידע		**מס׳ הנוהל:** 5.2	**עדכון מס׳:** 5
תאריך נוהל קודם: 31/3/25	**תאריך עדכון:** 7/5/26	**דף מס׳:** 1	**מתוך:** 8

מהות העדכון:

גרסה מס׳	מהות העדכון	תאריך
1	עדכון נוסחים ומחיקת דוגמאות לא רלוונטיות של אתרים בהם אין לגלוש	9/1/20
2	שינוי תדירות החלפת סיסמאות ומורכבות הסיסמא	13/1/22
3	בדיקה ואישור מחדש	4/12/22
4	עדכון מהדורת תקן חדשה	31/3/25
5	תיקוף הנוהל והוספת הנחיות עבודה בכל הקשור לשימוש ב-AI	8/1/26
6	שילוב שם המנכ״ל החדש	7/5/26

1. מטרת הנוהל

להתוות ולהגדיר מדיניות אבטחת מידע לתאגיד מי רמת גן שינחיל הנחיות אבטחת מידע בתאגיד.

2. הגדרות

2.1. תאגיד – תאגיד מי רמת גן.

2.2. מדיניות אבטחת מידע – מסמך ארגוני פומבי המתווה את תפיסת הארגון והנחיות ההנהלה בדבר אבטחת המידע בתאגיד.

2.3. ניהול זהויות - תמונת ההרשאות בדגש על מידע מיידי לגבי הרשאות הגישה שיש לכל עובד.

2.4. התממת נתונים – יצירת עותק של מאגר נתונים שממנו הושמטו או הוסוו פרטים מזהים, כדי לאפשר מסירה של מאגר נתונים זה לגורם חיצוני, בלי לסכן את שמירת הסודיות של הנתונים .

3. תוכן הנוהל

3.1. תאגיד מי רמת גן יגדיר מדיניות אבטחת מידע בארגון. המדיניות תציג את תפיסת ההנהלה בנושא אבטחת המידע בתאגיד ואת מחויבותה לנושא.

3.1.1. הנהלת מי רמת גן תשתף את עובדיה באמצעות ישיבות צוות היגוי וגורמים מוזמנים נוספים (מסמך ישים 1) בגיבוש המדיניות בתחום אבטחת המידע.

3.2. ההנהלה תפרסם בקרב כלל עובדי התאגיד את מדיניותה בתחום אבטחת המידע על גבי מנשר ובחתימתה. המנשר יופץ בדוא״ל לעובדים (נספח 1).

3.2.1. המנשר יהיה זמין לכלל הציבור על גבי לוח המודעות/ אתר האינטרנט ועותק יימסר לכל דורש.

3.3. מדיניות אבטחת המידע בתאגיד מי רמת גן תקבע עקרונות מנחים בנושא אבטחת מידע ותשמש כבסיס לפיתוח בקרות אבטחת מידע ולכתיבת נהלי אבטחת המידע.

3.4. הנהלת מי רמת גן תשאף להגברת המודעות בקרב העובדים, הקבלנים, הלקוחות והציבור בכלל לשמירה על כללי אבטחת המידע.

3.5. <u>פעולות לשמירת מערכת ניהול אבטחת המידע</u>

3.5.1. תאגיד מי רמת גן יקיים מערכת ניהול אבטחת מידע לפי דרישות התקן ISO 27001:2022 בשילוב עם מערכת ניהול בטיחות ובריאות תעסוקתית ISO 45001, מערכת ניהול סביבתי ISO 14001 ומערכת ניהול איכות ISO 9001:2015.

3.5.2. תאגיד מי רמת גן ישאף לקדם מדיניות אבטחת מידע, לשמור על כללי אבטחת המידע בהתאם לחוקים ולתקנות במדינת ישראל ובהתאם לדרישת הרשויות הממונות על אבטחת מידע תוך נקיטת כל האמצעים למניעת נזקים ללקוחות, תושבי רמת גן, בעלי העסקים בעיר, עובדי התאגיד, ספקים, קבלנים והציבור בכלל.

3.5.3. ההנהלה תקצה משאבים ואמצעים נדרשים, בהתאם לתקציב וסדרי העדיפויות, לצורך הפעלה תקינה של מערכת ניהול אבטחת מידע ובכלל זה הן משאבים חומריים והן משאבים אנושיים.

3.5.4. ההנהלה תקבע יעדים בתחומי אבטחת המידע ותפעל להשגתם, לשיפורם ולעדכונם מדי תקופה (מסמך ישים 2).

3.5.5. ההנהלה תקיים תהליך של ניטור ובקרה אחר השגת היעדים בתחום אבטחת המידע. יבוצע ניטור תקופתי וסקר סיכונים באתרים ובמערכות המידע שיקבעו ע״י מנהל מערכת אבטחת המידע בתאגיד, ינותחו סיבות לחריגות ויבוצעו פעולות תיקון ומניעה על מנת להקטין את רמות הסיכון לאבטחת המידע הארגוני.

3.5.6. תאגיד מי רמת גן יפעל לשיפור מתמיד של מערכת אבטחת המידע ויתאים עצמו להתפתחויות הטכנולוגיות המשליכות הן על האיומים והן על ההגנות הנוגעות למערכת אבטחת המידע לרבות עמידה בדרישות הישימות הנוגעות לאבטחת מידע.

3.5.7. הנהלת תאגיד מי רמת גן תכלול שיקולים של אבטחת מידע בתהליכי פיתוח תשתיות המים והביוב ובתהליך מתן שירותים ללקוחות ובהתקשרויות עם ספקים בשאיפה לצמצם השפעות שליליות של אבטחת מידע.

3.5.8. תאגיד מי רמת גן יפעל בשיתוף פעולה עם הרשויות הממונות, עם הלקוחות והספקים בכל ההיבטים הנוגעים לאבטחת מידע.

3.5.9. אבטחת המידע היא מעניינו של כל עובד בתאגיד מי רמת גן ובאחריותו של כל אחד הממלא תפקיד בתאגיד.

3.6. הנחיות הנהלת התאגיד וחברת המחשוב החיצונית בנושא אבטחת מידע לעובדים הן:

3.1.1. הרשאות כניסה למערכת:

3.1.1.1. שימוש במחשב מותנה בהזדהות (שם משתמש וסיסמא) של המשתמש בכניסה למחשב.

3.1.1.2. הרשאות יוענקו לעובד עפ״י הנחיצות בגישה למידע לשם מילוי תפקידו בהתאם לניהול זהויות ולא באופן גורף.

3.1.1.3. מתן/ביטול של הרשאות נוספות תועברנה לאחראי המחשוב דרך הממונה.

3.1.1.4. אחת לשנה תבוצע סקירת הרשאות למערכות השונות.

3.1.2. יש לכבות את המחשב בסוף כל יום, כיבוי המסך אינו מספיק, יש לכבות את המחשב עצמו.

3.1.3. חל איסור על הבאת מדיות (CD, דיסק, DVD וכו׳) והכנסתם למחשב.

3.1.4. אין להוציא מדיות מהארגון ללא קבלת אישור.

3.1.5. אין למסור את סיסמת המחשב שלכם לכל גורם שהוא, עליכם להפעיל שיקול דעת גם כשמדובר במסירת הסיסמה לעמית מהעבודה, זכרו שסיסמה זאת עלולה לשמש אותו לביצוע פעולות ״לא כשרות״ בשמכם ! ניתן – תמיד – לבקש מחברת המחשוב לשנות את הסיסמה.

3.1.6. הודעה בגין שינוי סיסמת המחשב תופיע כל 90 יום יש לשנות לסיסמאות בעלות לפחות 8 תווים מורכבים וביניהם סימן מיוחד, אות גדולה ואות קטנה. אי שינוי הסיסמא יוביל לנעילת המחשב .

3.1.7. השתלטות מרחוק על המחשב מיועדת עבור חברת המחשוב – ״נטקור״ בלבד ואין לאפשר לשום גורם אחר גישה לאפשרות זאת ללא קבלת אישור.

3.1.7.1. בכל מקרה של השתלטות מרחוק, עובד התאגיד שנעשית השתלטות על מחשבו, יפקח אחר התהליך לכל אורכו.

3.1.8. יש להיות ערניים לגביי וירוסים שמגיעים דרך הדואר

3.1.8.1. יש לפתוח מייל אך ורק אם אתם מצפים לדואר הזה וברור לכם מקורו ונושאו.

3.1.8.2. לא לפתוח מיילים ללא שם השולח.

3.1.8.3. לא לפתוח אם שם השולח לא מוכר.

3.1.8.4. לא לפתוח אם בשם השולח רשום השם שלכם.

3.1.8.5. לא לפתוח אם נושא המייל לא מובן.

שם הנוהל: מדיניות אבטחת מידע		**מס׳ הנוהל:** 5.2	**עדכון מס׳:** 5
תאריך נוהל קודם: 31/3/25	**תאריך עדכון:** 7/5/26	**דף מס׳:** 4	**מתוך:** 8

3.1.8.6. לא לפתוח אם הנושא לא אופייני לשולח (למשל: מכתב שכותרתו: "אני אוהב אותך" והוא הגיע מספק הציוד המשרדי שלכם – יש להניח שזה וירוס.(.....

3.1.8.7. לא לפתוח דואר שצורף לו קובץ (תמונה, מכתב WORD וכו׳) אלא אם יודעים בוודאות מה תוכנו, אתם מזהים את סוג ומהות הקובץ וציפיתם בדיוק לו.

3.1.9. מדיניות אבטחת המידע בארגון מונעת משיכת מיילים מתיבות דואר "פרטיות" (כולל ובמיוחד שרתי דואר "חינמיים" כ Gmail, Hotmail שאינן מנוהלות בשרת הדואר שלכם)

3.1.10. כל מייל שיוצא מהארגון נשמר על שרתים שונים בדרך ליעד וניתן בקלות יחסית לקרוא את תוכנו ולעשות בו שימוש, שימו לב למה שאתם כותבים או שולחים החוצה!

3.1.11. במשרד מותקנות מערכות הגנה מפני וירוסים וחדירה לא מורשת, מערכות אילו אינן מגינות על המחשבים הניידים שלכם בעת שהם מחוץ למשרד, יש נקוט משנה זהירות בעבודה מחוץ למשרד.

3.1.12. מדיניות אבטחת המידע בארגון מונעת גישה לאתרים שלא לצורכי העבודה וחל איסור מוחלט לגלוש לאתרים לא מוכרים ומפוקפקים, יש לזכור כי מעבר להיבט המשפטי/תדמיתי (כניסה – למשל – לאתר פורנוגראפי נרשמת ב"אינטרנט" ככניסה של הארגון לאתר הנ"ל !) אתרים כאלה עושים לעיתים שימוש בתוכנות ריגול ותקיפה.

3.1.13. מדיניות אבטחת המידע תמנע גישה לאתרים messenger, SKYPE ,Facebook או תוכנות דומות.

3.1.14. מסמכי עבודה חשובים: חובה לשמור אך ורק בשרת בספריה שהוקצתה לכם, קובץ שלא ישמר בשרת – לא יבוצע לו גיבוי והוא עלול להימחק או להינזק – ללא יכולת שיחזור!

3.1.15. אין להתקין תוכנות במחשב, כולל תוכנות מהאינטרנט (כגון בבילון וכו׳) וכולל תוכנות המבקשות להתקין את עצמם בזמן שאתם גולשים או מקבלים דואר. כל זאת על מנת שנוכל לוודא שהתוכנה לא פוגעת במשאבי הרשת ולוודא שאין צורך ברישיון לתוכנה.

3.1.16. יכולת הגישה של החברה לאינטרנט מוגבלת, חובה להקפיד לסגור את הגלשן כאשר סיימתם לגלוש, אין לעבוד בריבוי חלונות גלישה, הימנעו מאתרי וידאו או מוסיקה והורידו תוכנות – אך ורק לצורכי עבודה ורק לאחר קבלת אישור.

3.1.17. שליחת דואר לרשימת תפוצה של כמה עשרות נמענים ויותר, עלולה לגרום ל"סימון" העסק כשולח דואר ספאם וכתוצאה מכך לחסימת כל הארגון ומניעת האפשרות לשלוח מיילים ממנו, במידה ושליחה כזאת היא צורך ממשי – יש לתאם זאת עם ספק האינטרנט.

3.1.18. בשל מגבלות מקום יש להקפיד למחוק ב OUTLOOK שלכם כל מופע מיותר כמו: פגישות שכבר עבר זמנם, דואר שקיבלתם וכבר קראתם, דואר יוצא שהעתק ממנו נשמר בתיבת הדואר היוצא וכו׳. אין לעשות שימוש אישי בדואר האלקטרוני – אלא עסקי בלבד.

3.1.19. אין לבצע העברות מקום של מחשב או חלקי מחשב ללא קבלת אישור.

3.1.20. אין להוציא חלקי מחשב מהארגון ללא קבלת אישור.

3.1.21. בכל מקרה של אובדן או גניבת מחשב יש להודיע באופן מיידי לממונה אבטחת מידע בתאגיד ו/או לחברת המחשוב (נטקור).

3.1.22. בכל תקלה ובמידה ואיש חברת המחשוב מחברת "נטקור" לא באתר, ניתן לפנות במייל ל-Yaron@net-core.co.il או במידה והתקלה דחופה: ניתן לפנות למוקד שרות של "נטקור פתרונות תקשורת בע"מ" בטלפונים: 054-4404114 03-6327722 והתקלה/בעיה תטופל.

3.1.23. כל חריגה מנהלים אלא דורשת אישור בדרג מנכ"ל/סמנכ"ל ותבוצע על ידי אנשי "חברת נטקור בלבד".

3.1.24. <u>שמירה על חיסיון הנתונים</u>:

3.1.24.1. אסור למסור מידע המוגן מחוק צנעת הפרטת אלא אם יש צו בית משפט או אישור חוקר משטרה.

3.1.24.2. מידע מוגן הוא למעשה כל מידע המכיל מידע אישי כגון תעודת זהות, שם, כתובת, טלפון, חשבון בנק וכרטיס אשראי וכו׳.

3.1.24.3. משתמש הנמצא בספק לגבי חומר מסוים, חייב לבדוק זאת באמצעות היועץ המשפטי או הממונה עליו לפני ביצוע פעולה שכזו.

3.1.24.4. באחריות כל עובד שברשותו מחשב PC, עם עזיבתו את עמדת המחשב לבצע שמירה ולצאת מהמערכת באופן מסודר, הכולל סגירת כל היישומים הפעילים.

3.1.25. <u>שמירת נתוני כרטיסי אשראי</u>:

3.1.25.1. עובדי התאגיד הנחשפים לפרטי כרטיסי אשראי של לקוחות ישמרו על סודיות הנתונים ולא יבצעו בהם שימוש שאינו מורשה.

3.1.25.2. לאחר הזנת נתוני האשראי במערכת הגבייה, יש למחוק את מספר כרטיס האשראי מלבד 4 ספרות אחרונות.

3.1.25.3. אין לשמור ו/או להעביר נתונים של מספר כרטיס האשראי מלבד 4 ספרות אחרונות.

3.1.25.4. אין להעביר ו/או לשמור נתונים מלאים של מספר כרטיס האשראי בשום אמצעי תקשורת (דוא"ל/ פקס/ מסרון/ קובץ ממוחשב או מודפס).

3.2. <u>הנחיות עבודה בכל הקשור לשימוש ב-AI</u>:

3.2.1. שימוש ב-AI יעשה בהתאם לכל דרישות החוק והתקנות הרלוונטיות לרבות תיקון 13 לחוק הגנת הפרטיות (מסמך ישים 4).

שם הנוהל: מדיניות אבטחת מידע		**מס׳ הנוהל:** 5.2	**עדכון מס׳:** 5
תאריך נוהל קודם: 31/3/25	**תאריך עדכון:** 7/5/26	**דף מס׳:** 6	**מתוך:** 8

3.2.2. שימוש ב-AI לעובדי התאגיד יורשה רק לצרכי עבודה ולאחר קבלת אישור ממונה. אין לאפשר גישה של כלי AI למערכות הארגון ללא אישור.

3.2.3. שמירה על סודיות, פרטיות ואבטחת נתונים. חל איסור על עובדי התאגיד לבצע UPLOAD של מידע ארגוני למערכת AI. אין להזין או לשתף מידע דיסקרטי (כגון, מסמכים המכילים פרטים אישיים של אנשים כמו קורות חיים ועוד) באמצעות מערכות בינה מלאכותית אלא אם כן קיבלתם הרשאה לכך במפורש.

3.2.4. מניעת העלאת נתונים אישיים:

3.2.4.1. חל איסור מוחלט על העלאת נתונים אישיים של לקוחות או תושבים לסביבת ה-AI.

3.2.4.2. כל נתון אישי חייב לעבור תהליך התממת מידע לפני העלאתו למערכת AI .

4. מסמכים ישימים

4.1. מסמך ישים 1 – נוהל מס׳ 4.4 – ניהול מערכת אבטחת מידע

4.2. מסמך ישים 2 – נוהל מס׳ 6.2 – מטרות אבטחת מידע ותכנון להשגתם

4.3. מסמך ישים 3 – מסמך עמידה בדרישות הישימות – Annex A

4.4. מסמך ישים 4 - תיקון מספר 13 משנת 2024 לחוק הגנת הפרטיות, התשמ״א – 1981

5. אחריות ביצוע

5.1. מנכ״ל

5.2. ממונה על נושאי אבטחת המידע בארגון

5.3. מאמתת איכות ראשית

5.4. מנהל מערכות מידע

5.5. כל עובדי התאגיד

שם הנוהל: מדיניות אבטחת מידע		**מס׳ הנוהל:** 5.2	**עדכון מס׳:** 5
תאריך נוהל קודם: 31/3/25	**תאריך עדכון:** 7/5/26	**דף מס׳:** 7	**מתוך:** 8

6. נספחים

6.1. נספח 1 – הצהרת מדיניות אבטחת מידע

7. תפוצה

7.1. מנכ״ל התאגיד
7.2. ממונה על נושאי אבטחת המידע בארגון
7.3. מנהלי יחידות
7.4. מאמתת איכות ראשית
7.5. מנהל מערכות מידע
7.6. כל עובדי התאגיד

כותב הנוהל: *מכון אופק לניהול בע"מ*	***תפקיד:*** *יעוץ ארגוני, הנדסת תעשיה וניהול*
מנחה תהליך: דורון כתיב	*תפקיד : מנכ"ל*
מאשר הנוהל: דורון כתיב	***תפקיד:*** *מנכ"ל* ***תאריך:***

שם הנוהל: מדיניות אבטחת מידע		**מס׳ הנוהל:** 5.2	**עדכון מס׳:** 5
תאריך נוהל קודם: 31/3/25	**תאריך עדכון:** 7/5/26	**דף מס׳:** 8	**מתוך:** 8

נספח 1 -

מדיניות תאגיד מי רמת גן

בנושא אבטחת מידע
ISO 27001:2022

- *תאגיד מי רמת גן יקיים מערכת ניהול אבטחת מידע בהתאם לדרישות תקן ISO 27001: 2022.*
- *תאגיד מי רמת גן מחויב לאבטחת המידע של התאגיד לרבות מידע על תושבים, עובדים, קבלנים וספקים ומידע פנימי של התאגיד המשמש אותו בתהליכי מתן שירותי המים והביוב ובכלל.*
- *תאגיד מי רמת גן מחויב למלא את הדרישות עפ״י דין, הנוגעות לפעילותיו בנושא אבטחת מידע לרבות חוק חופש המידע וחוק הגנת הפרטיות.*
- *הנהלת תאגיד מי רמת גן תקצה משאבים ואמצעים נדרשים, בהתאם לתקציבה, לצורך הפעלה תקינה של מערכת ניהול אבטחת מידע. המשאבים כוללים הן משאבים חומריים והן משאבים אנושיים.*
- *תאגיד מי רמת גן יקדם הנחלת חינוך לאבטחת מידע לעובדים כחלק מהתרבות הארגונית לצורך שמירה על שלימות המידע ומניעת זליגתו.*
- *השמירה על אבטחת המידע היא מעניינו ובאחריותו של כל אחד מהמנהלים ועובדי תאגיד מי רמת גן.*
- *הנהלת תאגיד מי רמת גן תקבע יעדים בנושאי אבטחת המידע ותפעל להשגתם, לשיפורם ולעדכונם מדי תקופה.*
- *כדי להבטיח בקרה על השגת היעדים בתחום אבטחת המידע יבוצע ניטור תקופתי, סקר סיכונים, ניתוח הסיבות לחריגות ותבוצענה פעולות תיקון ומניעה להפחתת הסיכונים.*
- *תאגיד מי רמת גן יפעל לשיפור מתמיד של מערכת אבטחת המידע ויתאים עצמו לאיומים ולהגנות הנוגעות למערכת אבטחת המידע לרבות עמידה בדרישות הישימות הנוגעות לאבטחת מידע.*
- *תאגיד מי רמת גן יכלול שיקולים של אבטחת מידע בתהליכי אספקת שירותי המים והביוב ללקוחות בשאיפה לצמצם ולמנוע פגיעות באבטחת המידע.*
- *תאגיד מי רמת גן יפעל בשיתוף פעולה עם הרשויות הממונות, עם הלקוחות והספקים בכל ההיבטים הנוגעים לאבטחת המידע.*
- *הנהלת תאגיד מי רמת גן תביא לידיעת כלל העובדים, הקבלנים, הלקוחות ובעלי העניין האחרים את מדיניות התאגיד בתחום אבטחת המידע במטרה להבטיח את מודעותם להתחייבויות שלהם ואליהם בתחום אבטחת המידע.*

מר דורון כתיב – מנכ״ל

שם הנוהל: מדיניות אבטחת מידע		**מס׳ הנוהל:** 5.2	**עדכון מס׳:** 5
תאריך נוהל קודם: 31/3/25	**תאריך עדכון:** 7/5/26	**דף מס׳:** 9	**מתוך:** 8

מנכ״ל מי רמת גן