



ZINGER DANA & Co.

LAW OFFICES

זינגר דנה ושות'

משרד עורכי-דין

27 Keren Hayesod St. 27 רח' קרן חיסוד
 Jerusalem 94188 ירושלים
 Phone 02-6220990 טלפון
 Facsimile 02-6220999 פקסימיליה
jer@zinger-law.co.il

7 Metsada St. 7 רח' מצדה
 B.S.R 4 ב.ס.ר 4
 Bnei-Brak 5126112 בני ברק
 Phone 02-6220985 טלפון
 Facsimile 02-6220979 פקסימיליה
tlv@zinger-law.co.il

Shalom Zinger, Adv.
 Sarit Dana, Adv.
 Eyal Gur, Adv.
 Shani Singer, Adv.
 Yaniv Sapir, Adv.
 Neta Arbiv Ben-Gal, Adv.
 Liron Kanety, Adv.
 Tal Tsafrir, Adv.

Dr. Gadi Rubín, Adv.
 Ahaz Ben -Ari, Adv.
 Kobi Ivatsin, Adv.

שלום זינגר, עו"ד
 שרית דנה, עו"ד
 איל גור, עו"ד
 שני זינגר, עו"ד
 יניב ספיר, עו"ד
 נטע ארביב בן-גל, עו"ד
 לירון קנטני, עו"ד
 טל צפירי, עו"ד
 ד"ר גדי רובין, עו"ד
 אחז בן ארי, עו"ד
 קובי איבצן, עו"ד

ל"ט בטבת התש"ף
 16 בינואר 2020

לכבוד:

עו"ד אלעד מן – יועמ"ש עמותת הצלחה

פקס: 03-6114486 ובמייל: elad@man-barak.com

הנדון: מענה לבקשתכם לקבל מיזע לפי חוק חופש המידע ביחס לאבטחת מידע והגנת הפרטיות

סימוכין: מכתבכם מיום 17.11.2019

בשם פלג הגליל, החברה האזורית למים וביוב בע"מ (להלן: "פלג הגליל" או "התאגיד") הרינו להשיבכם כדלקמן:

1. בתאגיד ישנה פונקציה ייעודית שתפקידה הינו ממונה אבטחת מידע.

כתב מינוי מצורף ומסומן נספח א'

2. בתאגיד היו קיימים נהלי אבטחת מידע כל העת והוא פעל על פיהם.

בשנת 2017 וכחלק מהערכות התאגיד לכניסתו של התיקון שבוצע בתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 אשר נכנס לתוקף במאי 2018, שכר התאגיד שירותיו של יועץ מומחה בתחום אבטחת מידע וסייבר, מר עזרא דיין. יחד עמו גובשו נהלי אבטחת מידע מרוענניים והוכנו מצגות וטפסים ייעודים אשר הועברו לעובדים ונחתמו על ידם.

3. תנחלים והטפסים נחתמו בשנת 2017 ואילו המצגת הועברה לעובדים בסמוך לכניסת התקנות לתוקף בשנת 2018.

נוהל מאגרי מידע מצורף ומסומן נספח ב'.

נוהל מדיניות אבטחת מידע מצורף ומסומן נספח ג'.

מצגת לעובדים והתחייבות כי הבינו וקראו מצורפות ומסומנות נספח ד'.

דוגמת לטופס עליו חתומים כל עובדי התאגיד ועובדים חדשים שמצטרפים מצורף ומסומן נספח ה'.

4. התאגיד משתמש במספר תוכנות מחשב אשר כוללות מידע הנדרש לתאגיד לצורך מילוי ותפקידו על פי דין (לשם הדוגמה: מדידת צריכת המים וחיוב הלקוחות בהתאם, שירות לקוחות, מערכת ניטור ודיגום מים וכו'). בתוך כך, לתאגיד מאגר מידע רשום במשרד המשפטים כדין והוא כולל את כל המידע והנתונים מכלל המערכות חשונות.

שם המאגר: "קובץ פרטי צרכנים ונכסיהם"

מספר מאגר: 70002174

תאריך רישום המאגר: 1.3.2009 המאגר עודכן לאחרונה בשנת 2016.

סוג המידע הכלול בו:

מידע כלכלי – חובות.

מידע כלכלי – נכסים.

פרטי קשר.

קשרים משפחתיים.

מטרותיו:

ביצוע תפקידים ע"פ דין.

גבייה.

דיוור ישיר וקשר עם הלקוח.

טיוב נתונים.

מתן שירות ללקוחות.

ניהול מידע על תושבים ומתן שירות לתושב לשם מטרת הוואגיד.

אישור תרשום במאגר שנשלח אלינו בשעתו מהרשות למשפט טכנולוגיה ומידע (רמו"ט) מצורף ומסומן נספח ו'.

5. כמו כן, התאגיד התקשר עם חברת מחשוב בשם "מטרופולינט בע"מ", המספקת מערכות מחשוב לצורך ניהול צריכת המים, החיובים, מענה ללקוחות וכו' וכן אבטחת נתוני התאגיד. להלן תשובתו של מנזל אגף תשתיות בחברת מטרופולינט לעניין אופן שמירת הנתונים על גבי ענני מידע ושרתים :

"מטרופולינט מוסמכת לתקן אבטחת מידע ISO27001-2013 ומבוקרת באופן אחת לשנה כולל בדיקות תקפות הנחלים, אירועי אבטחה, ניהול אבטחת המידע בארגון ועוד.

בנוסף החברה אינה מחזיקת בכרטיסי אשראי ועובדת עם חברת סליקה מוסמכת PCI.

כל העובדים במטרופולינט חתומים על סודיות ומקבלים מידע שוטף בתחום אבטחת המידע".


תעודה מטעם מכון התקנים הישראלי המעידה על תקינות פעילות החברה מצורפת ומסומנת נספח ז'.

6. בנוסף, התאגיד עובד עם חברת "מילגם בע"מ" אשר מספקת לתאגיד שירותי צרכנות מים, שירות לקוחות וגבייה. החברה פועלת ומבוקרת על ידי מכון התקנים והיא מוסמכת ISO27001-2013 ועומדת בנהלי אבטחת המידע הנדרשים. כמו כן, כלל עובדיה חתומים על טפסים מתאימים.

תעודה מטעם מכון התקנים הישראלי המעידה על תקינות פעילות החברה מצורפת ומסומנת נספח ח'.

7. אנו זמינים לכל שאלה והבהרה נוספת.

בברכה,


נטע ארביב בן גל, עו"ד
יועמ"שית חתאגיד

העתיקים :

רו"ח אדי שוסב – מנכ"ל פלג הגליל

עו"ד ערן שטיינברג – ר"ענף וממונה תופש המידע בתאגיד.

מר נזיח סוויד – ממונה אבטחת מידע ואחראי תשונות מחשוב חיוניות בתאגיד.

נספחים

א



כ"א תמוז, תשע"ט
24 יולי, 2019

לכבוד
מר נזית סוויד
אחראי חדר בקרת

א.נ. שלום רב,

הנדון: כתב מינוי – ממנה תשתיות מחשוב חיוניות בארגון (תמ"ח)

- א. בהתאם לדרישות אבטחת המידע הארגוניות והרגולטוריות של תאגיד המים וחביב, הריני להודיעך כי מיום 24 יולי 2019 וינך הממונה והאחראי על התשתיות המחשוב החיוניות של התאגיד בכפוף לכל דין.
- ב. בהתאם לכך, מוטלת עליך האחריות למערכות המחשוב החיוניות ולדיווח על כל אירוע אבטחת מידע בהתאם לנחלי הארגון.
- ג. תוקף תמינויך שנה, מתחדש באופן קבוע.
- ד. איחולי הצלחה.

מל תלל
חברה תאורית למים וניזוב בע"מ
מור קטרוזה
מנהלת משאבי אנוש

בברכה,
מור קטרוזה
מנהלת משאבי אנוש

העתקים:

- רו"ח אדי שוסב- מנכ"ל
- אינג' עלי אבו ריש- ראש אגף הנדסה ופיתוח
- מר צביקה בינדר- מנהל מחלקת ביטחון תרום ותפעול



חברת האודית למים וביוזב בע"מ

נהלי מחשוב ואבטחת מידע

נוהל מאגרי מידע

1. כללי:

- 1.1. ביום ה- 11.3.1981, פורסט חוק הגנת הפרטיות, ותשמ"א-1981 (להלן: "החוק"). פרק ב' לחוק עוסק בהגנה על פרטיות במאגרי מידע ובהגדרות הרלוונטיות לחוק כגון "אבטחת מידע", "מאגר מידע", "מידע", "מידע רגיש", "מנהל מאגר", וסימן א' לחוק עוסק בין היתר בנושאים כגון חובת רישום מאגרי המידע בפנקס מאגרי המידע, זכות העיון במידע המוחזק במאגר המידע ובאחריות לאבטחת המידע שבמאגר המידע.
- 1.2. תקנות הגנת הפרטיות (תנאי הוזהקות מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו-1986 (להלן: "התקנות"), הינן תקנות אשר הותקנו מכוח החוק, וקובעות מגוון תחומים והנחיות עליהם יהיה אחראי מנהל המאגר בתחום אבטחת המידע כגון: עריכת רשימה מעודכנת של מורשי הגישה למאגר המידע לפי הרשאות הכניסה השונות, קביעת סדרי בקרה לגילוי פגיעות בשלמות המידע ותיקון ליקויים, הקמת קובץ נהלים שבפורטו אמצעי האבטחה, הדירגת התלפזת-סיסמאות, ניהול יומן אירועים חריגים וכו'.
- 1.3. החוק והתקנות, קבעו חלכה למעשה, את ההוראות הכלליות חדרושות לניהול מאגר מידע.
- 1.4. בחתום להוראות החוק והתקנות וחליטה הנחלת התאגיד למסד בנוהל את הליך ניהול ואבטחת מאגרי המידע המצויים בבעלות התאגיד.

2. מטרת ויעוד הנוהל:

למסד את הליך ניהול ואבטחת מאגרי המידע המצויים בבעלות התאגיד.
לקבוע את כללי ניהול אבטחת המידע ומידור המידע המצוי במאגרי המידע מפני משתמשים שאינם מורשים.

3. הגדרות:

- 3.1. "מנהל מאגר": מנהל פעיל של גוף שבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה;
- 3.2. "ממונה אבטחת המידע": אדם שמונה לממונה על אבטחת מידע לפי סעיף 17 לחוק או אדם שמנהל המאגר קבע כי הוא אחראי על אבטחת המידע שבמאגר המידע;
- 3.3. "בקרה לוגית": ניטור שוטף ממוחשב אחר הפעילות במערכת הממוחשבת, תוך התמקדות באירועים חריגים או רגישים.
- 3.4. "פיקוח לוגי": מעקב אחר פעילויות במחשב גם לאחר ביצוע הפעילות ובהשתיי זמן כלשהו.

4. מאגרי המידע שבבעלות התאגיד:

בהתאם למפורט בתקנות הגנת חפרטיות (אבטחת מידע), רמת האבטחה החלה על מאגר המידע שבבעלות התאגיד (המוגדר כגוף ציבורי) הינה בינונית. מאגר המידע כולל מידע אישי אודות 40,000 לקוחות התאגיד כגון: נתוני תקשורת, מידע על נכסי הלקוחות, פרטי תשלום וכיוצ"ב.

** במהלך שנת 2019 יבצע התאגיד תליך רישום למאגר בהתאם להנחיות הרשות למשפט, טכנולוגיה ומדע.

5. מורשי הגישה למאגר המידע:

מר אדי שוסב – מנכ"ל התאגיד ומנהל המאגר

צביקה בינדר – רע"ן ביטחון מיס ותפעול

מר עזרא דיין – ממונה אבטחת מידע מטעם התאגיד

(להלן: "מורשי הגישה" ו/או "המשתמשים")

6. תיאור התהליך:

6.1. הנחיות כלליות ליישום הנוהל:

6.1.1. מורשי הגישה למאגרי המידע יקפידו על יישומן המלא של הנחיות נוהל זה המתייחסות אליהם. ממונה אבטחת מידע יקבע ויפרסם את הפרמטרים לניהול מערכת הסיטמאות המחייבת את כלל המשתמשים, יפקח, יבקר ויאכוף את יישום הנוהל. קביעת כללי אבטחת המידע תבוצע בנפרד, עבור כל מערכת מידע המנוהלת מערכת סיטמאות אוטומטית.

6.1.2. מנהל המאגר וממונה אבטחת מידע ידאגו ליישם הנחיות נוהל זה, כל אחד בתחומו, כמפורט להלן. למען חסר ספק, ממונה אבטחת מידע יחיה כפוף לחוראות והנחיות מנהל המאגר, וכל הסמכויות המוקנות לממונה אבטחת מידע על פי נוהל זה יחיו מוקנות גם למנהל המאגר ו/או מי מטעמו.

6.1.3. מנהל המאגרים יודיע לרשם מאגרי המידע, בכתב, את שמו של ממונה אבטחת מידע במאגרים.

6.2. כללים לניהול מאגרי המידע ואבטחת המידע שבמאגרים:

6.2.1. אבטחת המידע במאגרים תתבסס על מנגנון האבטחה המובנה במערכות ההפעלה. יש לחפעיל את מירב האופציות שהמנגנון מספק.

6.2.2. לכלל המשתמשים יוקצה עם הצטרפותם, סיטמאות אישיות ורק על פיהן תתאפשר הגישה למאגרים.

6.2.3. כל אחד מהמשתמשים, ללא יוצא מן הכלל, יוגדר באופן אישי ותקבענה לו הרשאות הבלעדיות לו.

6.2.4. מנהל המאגר וממונה אבטחת מידע יחיו אחראים לקביעת הרשאות של המשתמשים. יישום הרשאות יבוצע על ידי מנהל המאגר בתיאום עם ממונה אבטחת מידע.

6.2.5. למען חסר כל ספק, מודגש כי ההרשאה איננה רק האפשרות הגישה למאגר מידע מסוים, אלא גם הגדרה מדויקת של הפעילויות שרשאי משתמש לבצע במאגר: אחזור ו/או עדכון ו/או תוספת ו/או מחיקה.

- 6.2.6. משתמש הפונה למאגר המידע, יתבקש להזדהות. רק במקרה שהזיהוי עבר בהצלחה, יקבל המשתמש על המסך את פרטי מאגר המידע אליו הוא רשאי לפנות. הרשימה לא תכלול מאגרי המידע שאינם בהרשאת.
- 6.2.7. זיהוי משתמש יהיה באמצעות שמו (USER ID). במקרה של בעיה בזיהוי המשתמש, תיחסם התקשורת ותוצג הודעה. רק מנהל המאגר או מורשה מטעמו, יוכלו לבצע שחרור חתסימה, אחרי שבדקו את המקרה לגופו.
- 6.2.8. לא יתאפשר מעבר ממאגר מידע אחד למשנהו, אלא דרך יציאה וכניסה מחדש באמצעות מערכת חסימאות.
- 6.2.9. באחריות מנהל המאגר לבדוק כל משתמש אחת לשנה, לצורך עדכון מפת ההרשאות הביצוע יהיה ביוזמת מנהל המאגר ובתיאום עם ממונה אבטחת מידע.
- 6.2.10. ממונה אבטחת מידע יוסיף או ינפה אנשים מן הרשימה רק בהתאם לפניה בכתב מטעם מנהל המאגר.
- 6.2.11. עזיבת משתמש וזינו החלטה על ביטול הרשאת, תועברו מידעיו ליוזעו ממונה אבטחת מידע, וזה יבטל את הרשאות הגישה של המשתמש.

6.3. זיהוי בסיסמא:

- 6.3.1. כל משתמש יוכל לגשת אך ורק אל מאגרים המותרים לו, תוך מזעור אפשרויות חשיפת סיסמאות האישיות. מעבר לזיהוי הפונה אל המערכת ע"י שמו, תתאפשר הפניה רק באמצעות סיסמא. הסיסמא תהווה את החוליה העיקרית בהגנה על הרשאות הגישה.
- 6.3.2. לכל המשתמשים יוקצו, עם הצטרפותם למאגר, סיסמאות אישיות ורק על פיהן תתאפשר הגישה למאגר. את הסיסמאות יקצה מנהל האבטחה. את סיסמאות הראשוניות יקצה מנהל האבטחה על פי הדרישה של מנהל המאגר הרלוונטי.
- 6.3.3. הסיסמא הראשונית תשמש לצורך כניסה ראשונית חד-פעמית למאגר המידע. עם כניסתו הראשונה לחשבון במערכת, על המשתמש להחליפה לפני כל פעולה אחרת. מכאן והלאה הסיסמא תוחלף ע"י המשתמש ובאחריותו.
- 6.3.4. הסיסמא לא תופיע על המסך בעת הקשתה.
- 6.3.5. חל איסור מוחלט למסור/לחשוף סיסמאות. אין לתלות את הסיסמאות על פתקיות בקרבת המחשב.
- 6.3.6. כגלגל, תוחלפנה סיסמאות אחת לשלושה חודשים. המערכת תכפה את החלפת הסיסמא על המשתמש. המשתמש יקבל התראה על מסך המחשב על סיום תוקף הסיסמא לפחות 7 ימים טרם פקיעתו.
- 6.3.7. במקרה של הקלדת סיסמא שגויה, תחסם התקשורת ותוצג על כך הודעה במסך. המערכת תאפשר שלושה ניסיונות כניסה, לאחר מכן תחסם התקשורת לחלוטין. חידוש הגישה של המשתמש אל המערכת יתאפשר רק אחרי קיומו של בירור ובקשת חידוש באמצעות מנהל המאגר. במקרה הצורך יועבר המקרה לידיעת הממונים הרלוונטיים.
- 6.3.8. עם כניסת נוהל זה לתוקף, תבוצע החלפה יזומה של סיסמאות כל המשתמשים, זאת על מנת להבטיח שלכל המשתמשים קיימות סיסמאות העונות להנחיות נוהל זה.
- 6.3.9. כל חריגה מהוראות נוהל זה, תתאפשר אך ורק לאחר פניה מנומקת בכתב ואישור בחתימה של ממונה אבטחת מידע ושל מנהל המאגר. כל המסמכים הללו יתויקו וישמרו בתיק מיוחד שיחיה אצל ממונה אבטחת מידע.

- 6.3.10. המשתמש יבחר סיסמא שתענה על הדרישות הבאות:
- 6.3.10.1. ככלל, הסיסמא תהיה קשה לניחוש.
 - 6.3.10.2. הסיסמא תהיה מורכבת משישה תווים (לכל הפחות) של אותיות, ספרות וסימנים.
 - 6.3.10.3. תו זהה לא יופיע בסיסמא יותר מפעמיים.
 - 6.3.10.4. לא יהיו יותר משלושה תווים עוקבים שיופיעו בסדר הרציף שלהם (א-ב', ספרות, סדר המקשים במקלדת וכו').
 - 6.3.10.5. אין להשתמש בסיסמא בעלת משמעות הקשורה באופן אישי למשתמש כגון: שם העובד, שם בן/בת זוג, מחלקתו, תאריכים בעלי משמעות וכדומה.
 - 6.3.10.6. אין לעשות שימוש במקשים פונקציונליים לאחסנת סיסמאות והפעלתן.
 - 6.3.10.7. אין לחזור על סיסמאות קודמות במשך 4 "דורות" האחרונים.
 - 6.3.10.8. אין להשתמש בסיסמא שהנה מילה חמופיעה במילון, בכל שפה שחיא.
 - 6.3.11. על מנת לאפשר תיקוני טעות בשלב קביעת הסיסמא, יש לאפשר הקלדה פעמיים.
 - 6.3.12. חל איסור מוחלט על מסירת סיסמאות. משתמש יתוודך על שמירת הסיסמא, אבטחתה ועל החובה שלא להעבירה לאחר. משתמש יתוודך להודיע מיידית על חשד של חשיפת סיסמתו.
 - 6.3.13. עליו החשד לחשיפת הסיסמא, יש להודיע על כך מיד לממונה אבטחת מידע ואו למנהל המאגרים. במקרה זה תיעשה פעולת מיידית לחלפתה וכן תיעשה בדיקה אודות אפשרות לשימוש בלתי מורשה בסיסמא.

6.4. הנחיות ביחס למורשי הגישה למאגרים:

- 6.4.1. מטרה. ניחול שוטף של חווי שאוונ במאגרי המידע בצורת מרכזית, תוך הפעלת שיקול דעת של מנהל המאגרים וממונה אבטחת מידע.
- 6.4.2. כדי לכלול משתמש ברשימת מורשי הגישה למאגרים, על ממונה אבטחת מידע להחתים את המשתמש על טופס "הצהרה והתחייבות שמירת סודיות", בו מתחייב המשתמש שלא להעביר לאנשים בלתי מורשים מידע שיקבל, או שימצא בידיו במסגרת עבודתו.
- 6.4.3. מנהל המאגר ירשום את המאגרים שאליהם יחיה המשתמש מורשה לגשת, יפריט אם המשתמש מורשה לעדכן את הנתונים או רק להציגם ויאשר בחתימתו על גבי הטופס את מתן הסיסמא והרשות לכניסת למאגר.
- 6.4.4. כל משתמש יוגדר בטבלאות החרשאה של המאגר. מנהל המאגר יעדכן את החרשאות על פי טופס ההצחרה על שמירת סודיות.
- 6.4.5. ממונה אבטחת המידע יעדכן את טופס ההצחרה ברשימת החרשאות וישמור אצלו את המסמך למעקב. כמו כן, יהיה ממונה אבטחת מידע מוסמך להפעיל את שיקול דעתו לגבי החרשאה המתבקשת, ובתאום עם מנהל המאגר, תשונה החרשאה במידת צורך.
- 6.4.6. ממונה אבטחת מידע יהיה מוסמך לבטל הרשאות למשתמשים שסיימו את עבודתם/התקשרותם עם התאגיד, וכן לבטל הרשאה למשתמשים (בהתאם לנתונים המתעדכנים במערכות החרשאות) ואו במידה ונעשה שימוש לרעה בהרשאות שניתנו להם.

6.4.7. מידי שישה חודשים תתבצע בדיקה של ההרשאות, ע"י ממונה אבטחת מידע. תוך תאום עם הנוגעים בדבר, ישונו או יבוטלו ההרשאות, במידת הצורך.

6.4.8. באחריות המשתמשים עצמם וכן מנהלי כלל המחלקות בתאגיד, להוויע על כל שינוי תפקיד, פרישה, סיום חתקשרות ו/או כל שינוי אחר, המחייב עדכון הרשאות של המשתמש, בנוסף לשינויים המתעדכנים במשאבי אנוש של התאגיד.

6.4.9. לא ייגש משתמש למידע שאין הוא מורשה לגשת אליו. עיין או שימוש במידע שלא על פי ההרשאה מהווה עבירה וינקטו כנגד המשתמש צעדים משמעותיים.

6.4.10. משתמש שהורשה לגשת למאגרי מידע, חייב לשמור את סיסמתו בסוד ולא לאפשר לאדם אחר לתשתמש בו. אם יתברר כי נעשה שימוש שלא כדין במידע תחת הסיסמא של משתמש מסוים, יישא המשתמש עצמו באחריות לכך.

6.4.11. משתמש שהורשה לגשת למאגרי מידע, חייב לנקוט בצעדים הדרושים כדי למנוע מאנשים אחרים גישה למאגר בעת שמוצג בו מידע. אין לחשאייר את מאגר המידע פתוח ללא השגחת העובד המורשה.

6.4.12. ניהול הרשאות הגישה וניהול תחום החצפנה ייעשו על ידי מנהל המאגר וממונה אבטחת מידע בלבד.

6.5. קביעת סדרי בקרה לגילוי פגיעות בשלימות המידע וזניקון ליקויים

6.5.1. ממונה אבטחת מידע יודא פעילותה התקינה של מערכת ה"לוגים" בשרתים עליהם מותקנים מאגרי המידע.

6.5.2. ממונה אבטחת מידע יטפל באירועים חריגים המטופלים באמצעות מערכת ה"לוגים".

6.5.3. ממונה אבטחת מידע יגדיר אירועים ופעולות חריגות או רגישות, בתיאום עם מנהל המאגרים, ובתאום עם כל הנוגעים בדבר. ההגדרה הנ"ל תכלול ניטיונות סרק לכניסה למאגרים וכן ניטיונות לבצע פעולות בלתי מורשות אחרות.

6.5.4. בשרתים עליהם מותקנים מאגרי המידע, יישמר LOG של כל הפעילויות באמצעות תוכנה ייעודית, לתקופה של שלושה חודשים אחרונים, לכל הפחות.

6.5.5. לממונה אבטחת מידע תינתן גישה לבחינת דוחות המערכת בהתאם לצורך. ייבדקו ניטיונות כושלים להציב סיסמא, שמות משתמשים לא פעילים שנעשה בהם שימוש וכדומה.

6.5.6. בבדיקה תהיה גם התייחסות לשעות ולמספר הכניסות של כל משתמש.

6.5.7. הגדרות הפעילויות החריגות היחידים והתוגדכן לפחות פעם בשנה.

6.5.8. ממונה אבטחת מידע יבדוק וינתח את ה"לוגים" באמצעות כלים ממוכנים אחת לשבוע ויעביר הממצאים החריגים באופן מיידי למנהל המאגרים.

6.5.9. ממונה אבטחת מידע, בתיאום עם מנהל המאגר ומנכ"ל התאגיד, יערוך בירור מיידי ודחוף לגבי הממצאים החריגים שאותרו ויישם פעילויות נגזרות כנדרש.

6.5.10. ממצאים המעידים על פעילויות חריגות שבוצעו בכוונת תחילה על ידי משתמשים, יועברו בדחיפות ובדיסקרטיות למנכ"ל התאגיד ויובילו לטיפול משפטי בהתאם.

6.6. הגנה הפיזית על אתרון וזניקונים במאגרים

- 6.6.1. מטרה – הנחיות להגנת פיזית על אחסון הנתונים ומערכות עיבוד הנתונים האוטומטית ועל תשתית הרבות מבנה, אמצעי תקשורת, מטופים ותשתית חשמל מפני סיכונים סביבתיים ופגיעות חיצוניות.
- 6.6.2. ממונה אבטחת מידע יודא פעילות התקנות של מערכת המצלמות ומערכת האזעקה המותקנות בחדרי השרתים של התאגיד בהם מותקנים מאגרי המידע של התאגיד. במידה והמאגרים מותקנים בענן ספקי מערכות המידע – יודא תקינות עם ספקי מערכות המידע באמצעות שאלון ו/או תצהיר חתום מטעם הספק.
- 6.6.3. ממונה אבטחת מידע ינחה את עובדי ספק המחשוב בנעילת חדרי השרתים, ארונות התקשורת וכל מתקן בו תתאפשר גישה למערכות הנתקשות, המחשוב או השרתים של התאגיד.
- 6.6.4. ממונה אבטחת מידע ינחה את חב' השמירה על משרדי התאגיד לבדוק את חדרי השרתים וארונות התקשורת כחלק משגרת הסיורים במשרדי התאגיד והנערכת לאחז' שעות הפעילות של התאגיד. חב' השמירה תדווח על כל פעילות חשודה לרבות גורמים שאינם מוכרים לעובדים על עמדות מחשבים של התאגיד או עובדים עם מחשבים ניידים במשרדי התאגיד לאחר שעות הפעילות.
- 6.6.5. מנהל המאגרים ינחל יומן רישום ומעקב בו תפורט מצבת הנתוכנה והחומרה הקיימת בתאגיד וממונה אבטחת מידע ינחל יומן רישום בנושא מצבת החומרה.
- 6.6.6. כל שינוי במצבת הנתוכנה והחומרה, לרבות גריעת ציוד, משלוחו לתיקון או הוספת ציוד חדש, יתועדו ביומן. כמו כן, יידרש לציין את מיקומו במשרד.
- 6.6.7. אין לרכוש חומרה או תוכנה ללא אישור טכני של ציוד החומרה על ידי ממונה אבטחת מידע.

7. אחריות, סמכות ותוקף:

- 7.1. נוהל זה אינו מחליף את דרכי התערבות והטיפול הקיימים במקרים המובאים לעיל, אלא בא להוסיף עליהם.
- 7.2. האחריות וחסימות לביצוע נוהל זה הינה בהתאם לאמור לעיל.
- 7.3. נוהל זה ייכנס לתוקפו החל מיום פרסומו.



1. כללי:

- 1.1. מטרת הנוהל לחגדיר את מדיניות פלג הגליל החברה האזורית למים וביוב בע"מ (להלן: "התאגיד") בנושאי אבטחת מידע ואת פעילויות המחשוב למניעה, תחזוקה וניהול משימות אבטחת מידע.
- 1.2. תחום אבטחת מידע בארגון הינו נרחב ורב גוני. תחום זה מרכז את המשימות שמבוצעות על מנת להבטיח שימוש ראוי במשאבי המחשוב של התאגיד, שמירה על אמינות המידע, שמירה על זמינותו, מניעת רוגלות, תדירות לא מורשות ווירוסים למיניהם, הדרכת המשתמשים לשימוש נכון ומאובטח בציד המחשוב, המידע ואמצעי האחסון בתאגיד.

2. מטרת ויעוד הנוהל:

- 2.1. הנוהל מיועד למשתמשי התאגיד, אנשי תפעול, כוננים, מפקחים, ספק מתן שירותי מחשוב, ספקי מערכות המחשוב ומערכות המידע של התאגיד, משתמשי התאגיד וכל גורם בתאגיד בעל גישה למערכות המחשוב. הנוהל מחייב כל גורם המטפל בשרתים בתאגיד ו/או בתחנות חבודה ו/או במאגרי חמידע.
- 2.2. הנוהל מציג תיאור הפעולות שיש לבצע בתחום אבטחת מידע לרבות בתחום תשתית, ניהול הרשאות וסיסמאות, טיפול באירועים, הפצת מדיניות ומניעה.

3. תיאור התהליך:

3.1. התקנת תוכנות לא מאושרות

- 3.1.1. התקנת תוכנה לא מאושרת תכלול בין היתר את הרכיבים הבאים;
 - תוכנה לא חוקית, תוכנה מועתקת ללא חרשאה או שנרכשה באופן אחר שלא בהתאם לתנאי הספק המורשה ולהנחיות התאגיד.
 - כל תוכנה אחרת (גם אם נרכשה כחוק ע"י העובד באופן פרטי) המותקנת ללא קבלת אישור מנמ"ר התאגיד.
- 3.1.2. השימוש בתוכנה לא מאושרת עלול לגרום לשיבושים במערכות המחשוב של התאגיד.
- 3.1.3. כל משתמשי תחנות עבודה שבמחשבם קיימת או שהותקנה תוכנה לא מאושרת מחויבים להודיע על כך לספק מחשוב ו/או יועץ המחשוב בתאגיד באמצעות הדוא"ל. היה ועובד מצא שתוכנה לא מאושרת כלשהי הינה חיונית לעבודתו חשופת עליו לפנות בדוא"ל למנמ"ר התאגיד – אשר יבצע חסרה, או שתבוצע רכישה באופן חוקי ע"י התאגיד, או שהתוכנה תקבל אישור התקנה ושימוש מן הגורמים המוסמכים.
- 3.1.4. במסגרת פעילות האחזקה השוטפת במחשבי התאגיד יהיה טכנאי המחשוב רשאי למחוק כל תוכנה לא מאושרת בעת טיפולם בחומרה או בתוכנה.
- 3.1.5. חאחריות לגבי השימוש בתוכנה לא מאושרת תחיה על המשתמש באופן אישי, גם כלפי התאגיד וגם כלפי גורמים חיצוניים.

3.2. התקנת תוכנות המורדות מהאינטרנט

התקנת תוכנות כאלה במחשבי התאגיד אסורה גם אם התוכנה מסוג Shareware ללא אישור מנהל המחשוב של התאגיד.

3.3. שימוש בדוא"ל

3.3.1. שימוש בדואר אלקטרוני שלא לצורכי עבודה:

שרותי הדואר האלקטרוני הינם לצורכי עבודה בלבד. למניעת דלף מידע אין להשתמש בשירותי הדואר האלקטרוני להעברת מידע שלא לצרכי העבודה. במקרים בהם נתקל עובד ו/או מנהל בחשד לשימוש שלא לפי הנחיות אלו עליו לפנות למנהל המחשוב בתאגיד.

3.3.2. קבלת דבר דואר מגורם לא ידוע:

במקרה בו משתמש מקבל דואר אלקטרוני עם צרופה מגורם לא ידוע עליו למחוק את ההודעה כדי למנוע העברת וירוסים וסוסים טרויאניים לתוך מחשבי התאגיד כמו כן עליו להודיע מיידית טלפונית למנהל המחשוב בתאגיד.

3.3.3. שימוש בדואר אלקטרוני פרטי:

על העובדים להשתמש בשירותי הדואר האלקטרוני של התאגיד בלבד. ותבצע חסימה מלאה של שימוש בשרותי דוא"ל פרטיים חיצוניים.

3.3.4. טיפול בספאם

- 3.3.4.1. מערכת סינון דואר אלקטרוני מנטרת באופן רציף כל העברת מידע מהתאגיד ואליה בדואר אלקטרוני ומאתרת מידע מסוג ספאם ויכולה לחסום אותו.
- 3.3.4.2. עם גילוי אירוע, מנחל המחשוב של התאגיד, יבדוק את נתוני האירוע על מנת לברר את הסיבה לחסימת ההעברה.
- 3.3.4.3. המערכת מבטלת את העברת המידע האסור ומבצעת את הפעולות הנאות:
 - העברת הודעת חסימה למנחל המחשוב של התאגיד בדוא"ל.
 - רישום לוג של האירוע במערכת סינון הדואר.
 - על כל אירוע של ניסיון להעברת מידע שנחסם ע"י מערכת סינון דואר אלקטרוני יבדוק טכנאי מחשוב את סיבת החסימה, במקרה של חסימת שווא ישחרר הטכנאי את הדואר החסום.

3.4. זיווח, גילוי וטיפול בעת הופעת וירוס בתחנת עבודה או התפרצות וירוסים

- 3.4.1. בכל גילוי וירוס בתחנת עבודה, מבוצעות פעולות לנטרל נזק ולמנוע התפשטות וירוס ברשת.
- 3.4.2. בכל תחנת עבודה מותקנת תוכנת אנטי וירוס ברשת המנטרת את פעילות התחנה באופן שוטף.
- 3.4.3. עם גילוי וירוס בתחנה, מציגה תוכנת האנטי וירוס הודעה מתפרצת על המסך המיועדת לייזע את המשתמש.
- 3.4.4. עם הופעת הודעה מתפרצת, יפעל המשתמש בהתאם להנחיות שלהלן:
 - 3.4.4.1. המשתמש יסגור את כל התוכנות הפעילות.
 - 3.4.4.2. המשתמש יבצע כיבוי מסודר של המחשב (Shut down)
 - 3.4.4.3. המשתמש יודיע טלפונית ומיידית על גילוי וירוס במחשבו למכרז השירות והתמיכה של התאגיד טלפונית.
 - 3.4.4.4. המחשב יישאר כבוי עד לבדיקתו על ידי אנשי המחשוב התאגיד.
- 3.4.5. גילוי וטיפול ראשוני בהופעת וירוס במערכות התפעוליות
 - 3.4.5.1. חמערכות התפעוליות פועלות בין היתר באמצעות בקרים תעשייתיים השולטים במתקני תשתיות מים וביוג.
 - 3.4.5.2. כאשר עולה חשד להופעת וירוס במערכות הבקרה, יש לנטרל מיידית את עבודת הבקר החשוד, לנתק את התקשורת בין הבקר לרשת ה-OT ולהעביר את פעילות התחנה לפיקוד ידני (ללא התערבות בקר).

3.4.6. פעולות אחראי אבטחת מידע בעת אירוע התפשטות וירוס ברשת הארגונית/ תפעולית:

- אחראי אבטחת המידע יגיע אל המחשב החשוד ויבצע בו את הפעולות הבאות;
 - בדיקת סטטוס של הווירוס או הקובץ החשוד כנגוע בוירוס.

- סריקת החומר ע"י שני מנועי אנטי וירוס לפחות. במידת הצורך, פירוק הדיסק הקשיח והעברתו למנחל המחשוב של התאגיד לצורך חמשך טיפול באמצעות חיבור של הדיסק לתחנת הלבנה לטיפול בחסרת חווירוס.
- החומר שנסרק ונמצא נקי יוחזר למשתמש.
- יעשה כל מאמץ לשמור על מירב החומר של המשתמש הנמצא על הדיסק הקשיח. יש לציין, באופן כללי לא אנוור להיות חומר חשוב על הדיסק הקשיח של המשתמש אלא בשרתי התאגיד באמצעות האפליקציות הייעודיות וספריית הקבצים ברשת.
- בדיקת עדכניות של מנוע התוכנה וחתומות - במחשב ועדכון במידת הצורך.
- סגירת התקלה במערכת דיווח תקלות מחשוב.
- חיבור מחדש של המחשב לרשת ממנה הוצא המחשב.
- מילוי ושיגור טופס דיווח על אירוע ווירוס בתחנת עבודה.

3.4.7. התנהלות בעת התפרצות וירוסים

- 3.4.7.1. על תחנות העבודה של המשתמשים מותקנת חבילת אנטי וירוס של חברת ESET.
- 3.4.7.2. הדרישה היא כי כל תחנת עבודה תעודכן באופן אוטומטי בגרסה העדכנית הקיימת לכל חבילה, בכפוף להמלצות ספק תוכנת האנטי וירוס.
- 3.4.7.3. נקודת המוצא צריכה להיות היא שהאנטי וירוס מעודכן לקובץ חתימות האחרון שיש, ושמוע האנטי וירוס הוא הגרסה האחרונה שיש.

זחו סדר הפעולות שיש לבצע כדי למגר וירוס במחירות האפשרית, גם במקרים שקיימת התפרצות של וירוס חדש ושהחבילות עצמן עדיין אינן מעודכנות בדרך הטיפול בו ואו הסרתו.

3.4.8. פעילות עדכון וטיפול בעת אירוע

- 3.4.8.1. כניסה יומית לכלי הניהול של התוכנה לבדיקת מצב הווירוסים בתאגיד - באחריות מנחל המחשוב של התאגיד.
- 3.4.8.2. לוודא שבכלי הניהול מוגדר שבעת התפרצות וירוסים (נקבע ע"פ כמות וירוסים ליחידת זמן) נשלח מייל לתפוצה המונאימה
- 3.4.8.3. בעת התפרצות וירוסים בתאגיד, אשר האנטי וירוס לא מצליח להתמודד איתם, כגון וירוס חזש, או שינוי של וירוס קיים, יש להפעיל סריקה ע"י יותר ממנוע אנטי וירוס אחד וזאת על מנת לזהות את הקובץ הפוגעני.
- 3.4.8.4. הקובץ שנוצר יישלח לספק התוכנה אשר יספק שירותי תמיכה בכל בעיות האנטי וירוס. הקובץ יועבר ליצרן אנטי וירוס. בהתאם לתקיפה יועבר קובץ חתימות חדש.
- 3.4.8.5. במידה ולא עוזר חוזרים על הפעולה.
- 3.4.8.6. במקרים מסוימים ההתפרצות חוזרת על עצמה לאחר שעות או ימים, מכיוון שחווירוס משנה התנהגות. (מוטציה של חווירוס). – במקרה זה נדרשת תמיכה של יצרן אנטי וירוס.

3.4.8.7. בעת פתיחת הקריאה אצל ספק התוכנה יש לקרוא לנציג מטעמם אשר אחראי ללוות את התהליך עד לפתרון.

3.5. הפצת אנטי וירוס

- 3.5.1. בתאגיד מותקנת תוכנת אנטי וירוס בתחנות העבודה והשרתים. זרך הפצתו של האנטי וירוס בארגון לתחנות העבודה וזיא באמצעות policy ארגוני. הפצת אנטי וירוס מתבצעת אוטומטית בכל מחשב בארגון, ברגע שמתחבר אל ה-Domain מקבל את עדכון האנטי וירוס המתאים לו.
- 3.5.2. במקרה של המצאות אנטי וירוס אחר יש לבצע הסרה בעזרת כלי ההסרה של הגרסה / התוכנה הקודמת.
- 3.5.3. אין להסיר אנטי וירוס מונחנה ללא אישור מנהל המחשוב בתאגיד.

3.6. הקשחת תחנת עבודה

- 3.6.1. פעילות זו תכליתה לבנות סביבת עבודה בטוחה בתחנות העבודה של משתמשי הקצה בתאגיד. הקשחת תחנה מתבצעת באמצעות הפעלת מדיניות קבוצתית ב AD.
- 3.6.2. הגדרות אשר מונעות גישה לא מאושרת לקובצי סיסטם, מונעות ממשתמשים לבצע שינויים לא רצויים להגדרות אבטחה, הגדרות אוטומטיות בהתקנת אנטי-וירוס בתחנות והגדרות קבועות של שרתי Proxy לגלישה באינטרנט
- 3.6.3. הקשחת תחנת עבודה תתבצע זרך Group policy objects - Active Directory. המטרה היא לבנות סביבת העבודה בטוחה למשתמשים, ללא חשש לפגיעה בצרכים היומ-יומיים.
- 3.6.4. יש כמה GPO שמגבילים הרשאות משתמשים בתחנות עבודה:
- 3.6.4.1. Default Domain Policy
 - 3.6.4.2. Restrictions
 - 3.6.4.3. יש לבצע שינויים ובחירת תגדרות המגבילים הרשאות המשתמשים ע"פ המוגדר console הניהול של המערכת.

3.7. ניהול סיסמאות והקשחת סיסמאות בארגון

- 3.7.1. אבטחת המידע ברשת מתבססת על זיהוי אמין של המשתמשים.
- 3.7.2. הסיסמאות מיועדות לאמת את זהות המשתמשים ברשת. על מנת לצמצם הסיכון של שימוש לרעה בסיסמאות המשתמשים, נקבעו כללים ליצירת הסיסמאות ואופן השימוש בהן.
- 3.7.3. סיסמאות הינן חכלי לחגן על חדירה למערכות ולמחשבי הארגון, למידור, למניעת ריגול, למניעת גרימת נזק, ולמניעת חשיפת מידע למי שאינו מוסמך לכך ולכן על הסיסמאות להיות מורכבות ועליהן להשתנות אחת לזמן קצרה כמוגדר להלן:
- 3.7.4. סיסמת עבודה - מחרוזת בת 6 תווים אישית המורכבת מאותיות וספרות לפי בחירת המשתמש.

- 3.7.5. סיסמא ראשונית - סיסמא חד-פעמית המונפקת ע"י טכנאי המחשוב למשתמש בחשבון חדש, או במקרה של שכחתי סיסמת עבודה המצריכה הנפקת סיסמא ראשונית חדשה.
- 3.7.6. משך זמן מרבי לתוקף סיסמה עבודה - פרק הזמן חמרכי שנקבע לשימוש בסיסמת עבודה הוא 6 חודשים מחווד יצירה
- 3.7.7. משך זמן מזערי למוקף סיסמת עבודה - אם קיים חשש לדליפת חסימא, משתמש רשאי ויכול להתליף סיסמתו גם לפני שחלפו 6 חודשים ממועד יצירתה, אולם לא יותר מהחלפת סיסמא פעם אחת ביממה.
- 3.7.8. היסטוריית סיסמאות - על מנת למנוע שימוש חוזר בסיסמאות קודמות, המערכת שומרת את היסטוריית הסיסמאות של המשתמשים וחוסמת שימוש בסיסמא שכבר נעשה בה שימוש בעבר.
- 3.7.9. סודיות הסיסמא - סיסמאות הן אישיות וחל איסור לגלותן לאחר.

3.8. תהליך יצירה וניהול סיסמאות

- 3.8.1. עם הקמת חשבון חדש למשתמש, תקבע ע"י מקים המשתמש סיסמא ראשונית באמצעותה יבצע המשתמש כניסה ראשונה לחשבון.
- 3.8.2. עם כניסתו לחשבון באמצעות הסיסמא הראשונית, תדרוש המערכת באופן אוטומטי מהמשתמש ליצור לעצמו סיסמת עבודה קבועה שתשמש אותו במשך 6 חודשים.
- 3.8.3. סיסמא זו צריכה כאמור להיות בת 6 תווים שונים זה מזה, צירוף של אותיות וספרות בלבד. אין לכלול בסיסמא תווי פיסוק וטימנים מיוחדים.
- 3.8.4. על המשתמש לזכור את סיסמת העבודה שלו ולא לשוט אותה במקום ובאופן שמישהו מלבדו יוכל לראותה.
- 3.8.5. לאחר 6 חודשים של שימוש בסיסמא, יידרש המשתמש (באופן אוטומטי ע"י המערכת) ליצור לעצמו סיסמת עבודה חדשה וסיסמתו הקודמת תבוטל.
- 3.8.6. במידה ומשתמש חושש שסיסמתו נודעה לאחר, יפנה למרכז השירות ויפנה קריאה מתאימה לאיפוס סיסמא או הקמת סיסמא חדשה. לאחר שיקבלה יחליפה בסיסמת עבודה חדשה.
- 3.8.7. חל איסור על שימוש בסיסמא קולקטיבית חמשמשת קבוצת משתמשים
- 3.8.8. מערכת בקרת אבטחת המידע מפקחת באופן רצוף על כל פעילות חסימאות, מתעדת ומתריעה על כל הפרה של הכללים. על אירועי הפרה של כללי הסיסמאות יש לעדכן את מנחל המחשוב של התאגיד.
- 3.8.9. המטרה היא לבנות סיסמאות מורכבות המכילות: אותיות גדולות, קטנות, מספרים וטימנים. חסימא תכיל לפחות 6 תווים (לדוגמה: @12sdAbs)
- 3.8.10. לאחר קבלת החלטה לגבי מדיניות הסיסמאות, אפשר לשנות את ה-default domain policy ולאפשר קיום של סיסמאות ב-domain רק ב-complexity pattern.
- 3.8.11. לפי המדיניות אפשר גם לקבוע תוקף לסיסמאות. כל פרק זמן נתון, חודשיים למשל, המשתמש חייב לשנות את סיסמתו לחדשה שלא השתמש בה בעבר. הגדרה זאת נמצאת גם ב-GPO default domain policy.

3.9. ניהול משתמשים ותרשאות (בכפוף לנוהל קליטת ועזיבת עובד)

3.9.1. יצירת משתמש חדש ברשת

3.9.1.1. קבלת בקשה ואישור להוספת משתמש וחיבורו לרשת.

3.9.1.2. יצירת המשתמש ב AD של הרשת.

3.9.2. עזיבת עובד וחשבונות לא פעילים

3.9.3. בעת עזיבת עובד יתקבל דוא"ל ממנהל משאבי אנוש המפרט פרטי המשתמש ותאריך עזיבתו.

3.9.4. טכנאי המחשב יעבירו את חשבונות המשתמש שעוזב למצב DISABLE. יודגש, כי אין למחוק

את החשבון מה- AD. תיבת הדואר של המשתמש תחסם.

3.9.5. עם סיום עבודתו של העובד יבוצע ייצוא של תיבת הדואר של העובד לקובץ PST והקובץ יגובה

כחלק מנוהל חגיגי של התאגיד.

3.9.6. כעבור 30 יום לאחר עזיבתו של העובד החומר של העובד יועבר לתיקיית Disabled Users.

3.10. אחסון מידע

3.10.1. משתמשי התאגיד נדרשים לאחסן מידע רב במסגרת עבודתם. מידע לאחסן בשרתי הקבצים /

שרתי ניתוח המסמכים של התאגיד בלבד לאחסן בשרתי התאגיד בלבד.

3.10.2. ע"פ צורך ניתן לאחסן מידע במחשב המקומי או על גבי disk on key שנופק ע"י טכנאי

המחשב של התאגיד בלבד.

3.10.3. כמו כן יתכן צורך להשתמש במדיה מגנטית כדוגמת דיסק צרוב ודיסק קשיח.

3.10.4. אין להוציא מדיה מגנטית מחוץ לתחומי התאגיד (דיסקים קשיחים, דיסקטים וכו').

3.10.5. בעת שליחת מחשב לתיקון במעבדת חוץ, יש להקפיד להוציא את הדיסק הקשיח מהמחשב.

במקרה של דיסק תקול, יש להעבירו לצוות המחשוב לצורך השמדת המדיה.

3.11. טיפול שוטף ברשת המחשוב של התאגיד

3.11.1. במקרה של גילוי וירוס - הקובץ יימחק. דיווח על גילוי וירוס מבוצע ע"פ נוהל טיפול

בווירוסים.

3.11.2. במקרה של זיהוי קובץ כדוא"ל - SPAM, הקובץ יימחק ללא הודעה כלשהי. במידה וקיים

רצף הודעות SPAM שמקורן באותו המפיץ, נחסם המקור השולח על ידי מערכת סינון דואר

אלקטרוני.

3.11.3. במקרה של סוג קובץ אסור בכניסה לרשת – ונבוצע מחיקה של הדוא"ל עם קובץ חצרופה, ללא

הודעה על ידי מערכת FW העירונית.

3.11.4. במקרה של קובץ גדול החמורשה - וידווג עם הנמען בתאגיד שזוהא מצטוו לקבל את הקובץ

שנעצר בהסגר.

3.11.5. קובץ שהמגבלה היחידה שלו הוא גודלו ושהנמען שלו מצפה לו, ישוחרר לנמען.

4. אחריות, סמכות ותוקף:

- 4.1. נוהל זה אינו מחליף את דרכי ההתערבות והטיפול הקיימים במקרים המובאים לעיל, אלא בא לחוסיף עליהם.
- 4.2. האחריות והסמכות לביצוע נוהל זה הינה בהתאם לאמור לעיל.
- 4.3. נוהל זה ייכנס לתוקפו החל מיום פרסומו.



נהלי מחשוב ואבטחת מידע
נוהל מדיניות אבטחת מידע

נספחים

נספח א' - תקציר הנחיות משתמשי התאגיד בעבודת עם משאבי המחשוב

1. השימוש במחשב ובמאגרי המידע של התאגיד חנו לצורך עבודה בלבד וכפוף לנוהלי התאגיד.
2. יש להקפיד על שימוש בסיסמאות, חסיסמא היא אישית ואסור להעבירה לאחר.
3. חל איסור להתקין תוכנות שלא באישור מנהל המחשוב של התאגיד.
4. חל איסור להתקין רכיב חומרה פרטי מכל סוג שלא באישור מנהל המחשוב של התאגיד.
5. לידיעתך, כל המידע ופעילות מערכות המחשוב של התאגיד, מנוטרים ומבוקרים על ידי גורמי אבטחת המידע.
6. אין להשתמש במדיה ואמצעי אחסון חיצוניים שאינם שייכים לתאגיד.
7. אין להוציא חומרים מסווגים לרבות מדיה מגנטית מחוץ לאתרי התאגיד.
8. יש להתחבר לרשת המיועדת לעבודתך בלבד.
9. אין להשאיר חומרים פתוחים ונגישים למי שאינו מורשה, סגור ונעל כל מידע לרבות אבטחה פיזית.
10. בכל מקרה של תקלה או בעיה יש לפנות למרכז התמיכה לפתרון תקלות מחשוב טלפונית או באמצעות דוא"ל.
11. אין להשאיר בשום מקרה מחשב נייד ברכב ללא השגחה.
12. יש לצאת מחרשת בסוף חיום, אין לכבות את המחשב.
13. שימוש בציוד קצה (מדפסות, סורקים, מצלמות וכדו') לצרכי עבודה בלבד.
14. יש להקפיד על הדפסה דו-צדדית ככל הניתן.
15. יש להתחבר לרשת התאגיד מרחוק באמצעות נייד ומודם, עפ"י הנחיות ספק המחשוב של התאגיד בלבד.

נספח ב' - הדרכה והתחייבות למדיניות אבטחת מידע

1. אינטרנט

חשימוש באינטרנט הינו לצרכי עבודה בלבד. בשום אופן אין לבצע שימוש בעייתי בגלישה באינטרנט כגון: גלישה באתרי הימורים, פורנוגרפיה, פרסום מידע בעייתי באינטרנט (כגון כתיבת תגובות ופוסטים פוגעניים), ניסיונות לעקוף בקרות אבטחת מידע וכד'. קיים ניטור תמידי לגלישה באינטרנט.

2. דואר אלקטרוני

- 2.1. הדואר האלקטרוני הינו לשימוש צרכי עבודה בלבד.
- 2.2. יש לנקוט זהירות מרבית בעת שליחת דואר אלקטרוני כך שלא יועבר מידע רגיש אל גורם אשר אינו זקוק לו.
- 2.3. פרטיות הדואר מוגבלת, על העובד לדעת שבכל עת ניתן לגשת אל תיבת הדואר שלו בהתאם לצרכי הארגון והחוק.
- 2.4. אין לשלוח הודעות לנמענים אשר אינם מעוניינים בכך.
- 2.5. אין לשלוח הודעות שרשרת.
- 2.6. אין לשלוח הודעות תוך התחזות לאחר.
- 2.7. הודעות דואר חשודות יש למחוק מיידית ולדווח למנהל המחשוב של התאגיד.

3. רשת

- 3.1. ברשת המחשוב של התאגיד קיים מידע רב. כל עובד נדרש לשיקול דעת ואסור לו לנסות לגשת למידע אשר אליו יש לו הרשאות אך מאידך אין זה מעניינו.
- 3.2. מידע ארגוני יש לאחסן על רשת המחשוב. מידע אשר נמצא על הדיסק הקשיח המקומי אינו מגובה.
- 3.3. בסוף יום עבודה יש לצאת מהרשת ע"י ניתוק המשתמש מתרשת בלבד (לא לכבות את המחשב).
- 3.4. ניתוק זה מתבצע ע"י לחיצה על מקש התחל ובחירת בניתוק של המשתמש

4. רשתות אלחוטיות

- 4.1. כאשר כרטיס הרשת האלחוטית אינו בשימוש עליו להיות במצב של "DISABLE".
- 4.2. אין לנסות להתחבר לרשתות אלחוטיות זרות.
- 4.3. אין להתחבר לרשת אחרת / אינטרנט מהיר במקביל לחיבור לרשת של התאגיד.

5. מחשבים ניידים

- 5.1. אין להשאיר מחשבים ניידים ללא השגחה במקום ציבורי.
- 5.2. אין להשאיר מחשבים ניידים ברכב.
- 5.3. מחשב נייד אשר נשאר בתאגיד בזמן יום עבודה עליו להינעל בתוך ארון.

5.4. אין להתקין על המחשבים הניידים של החברה תוכנות לא חוקיות, תוכנות לשיתוף קבצים לדוגמא utorrent וכן אין לגלוש לאתרים לא ראויים (סקס, אלימות, הימורים) גם אם החיבור לאינטרנט נעשה שלא ברשת החברה, שכן אתרים אלו מכילים לרוב וירוסים וסוסים טרויאניים.

6. אחר

6.1. מיזע המאוחסן במערכות המידע של החברה הינו רכוש התאגיד.

6.2. שימושים לא אתיים בצידוד תמחשוב של התאגיד יגרור צעדים משמעתיים כנגד העובד.

הריני מאשר כי קראתי והבנתי את האמור לעיל והנני מסכים לכל.

שם	תאריך	חתימה

נספח ג' - דיווח על אירוע וירוס בתחנת עבודה

המקור הראשוני לאירוע

SOC	
דיווח משתמש	
מחלקת מחשוב	

(סמן X בתיבה המתאימה)

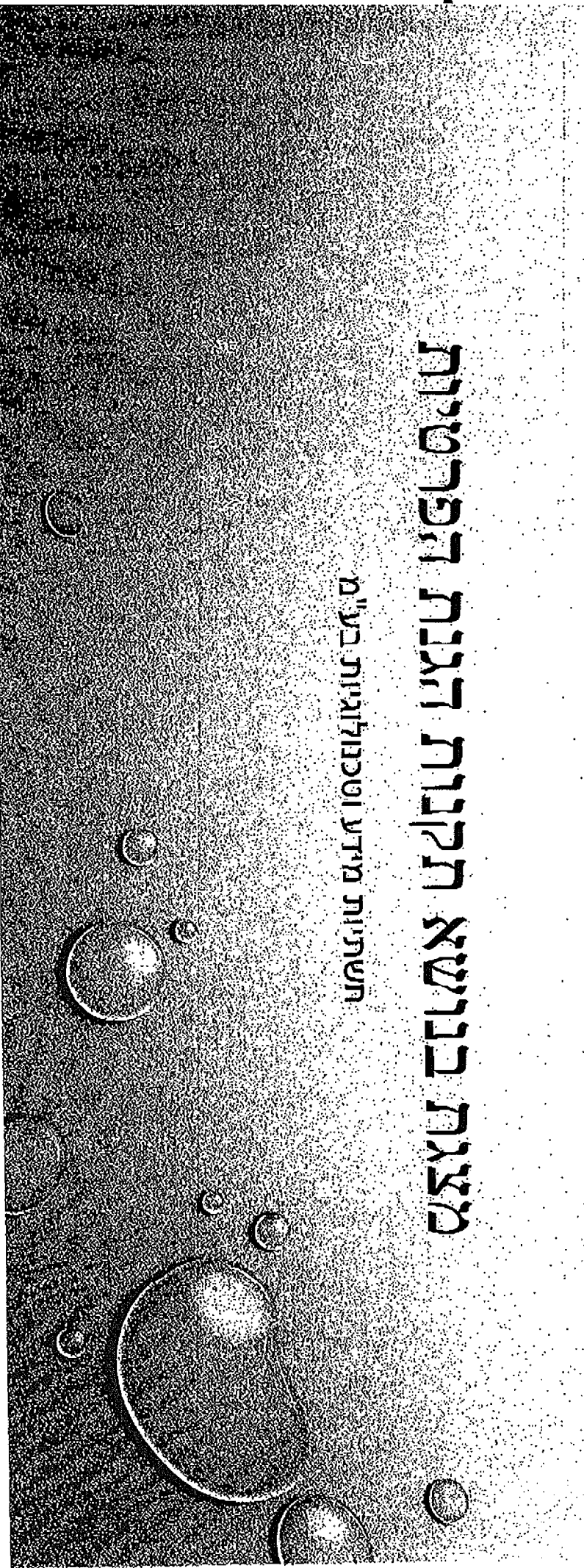
פרטי האירוע:

	עיתוי הגילוי
	זיהוי המחשב הנגוע
	שם המשתמש הפעיל בתחנה
	תיאור המדיה הנגועה
	סוג/שם הווירוס
	סטטוס התדבקה
	המלצות לפעולה
	סטטוס אירוע



מצגת בנושא תקנות הגנת הפרטיות

חברות מידע וטכנולוגיות בע"מ



תקנות הגנת הפרטיות

- ביום 21 במרץ 2017, אושרו בוועדת חוקה, חוק ומשפט של הכנסת תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "התקנות").
- התקנות הן שינוי מהותי ברגולציית אבטחת המידע בישראל, והן מטילות חובות משמעותיות על בעלי מאגרי מידע לאבטחת המידע שברשותם.
- בין החובות הכלולות בתקנות: אימוץ מדיניות מחייבת ונוהלי אבטחת מידע מקיפים, מינוי מערכות המידע בארגון וביצוע סקר סיכונים, הטמעת תפיסות אבטחת מידע בניהול כוח האדם בארגון וחופת דיווח על אירועי אבטחה. בנוסף, ביחס למאגרי מידע בעלי רגישות גבוהה, התקנות קובעות גם ביצוע מבדקי חדירות והטמעת אמצעי אבטחה.

רמות אבטחה שונות למאגרי מידע

- ככלל, התקנות יחולו על כל מאגר מידע שחייב ברישום לפי חוק הגנת הפרטיות. עם זאת, חלק מההוראות יחולו רק על מאגרי מידע ברמת אבטחה בינונית או גבוהה, אשר יהיו כפופים לנהלים מחמירים יותר.
- מאגרי מידע ברמת אבטחה בינונית כוללים, בין היתר, מאגרים הכוללים מידע רפואי, מידע על צנעת חייו של אדם, מידע על דעותיו הפוליטיות או אמונותיו של אדם, מידע ביומטרי, מידע כלכלי לרבות מידע על החגלי צריכה של אדם, וכן מאגרי מידע שנועדו לצורך דיוור ישיר.
- מאגרי מידע ברמת אבטחה גבוהה הם מאגרים הכוללים מידע רגיש כמפורט לעיל הכוללים פרטים על 100,000 אנשים ומעלה או שמספר חוזשי הגישה אליהם עולה על 100.

מסמכי מדיניות נהלים ובעלי תפקידים

- התקנות מחייבות כל בעל מאגר מידע לאמץ מסמך מדיניות המגדיר את מטרות המאגר, את סוגי השימושים בו, את הסיכונים העיקריים לפגיעה באבטחתו ואת דרכי ההתמודדות עמם.
- כל בעל מאגר מידע יחויב לקבוע נוהל אבטחת מידע בהתאם להגדרות מאגרי המידע שברשותו. הנוהל יחייב את כל עובדי הארגון ויתייחס, בין היתר, למיפוי מערכות המידע בארגון, ואבטחתן, למדיניות הרשאות הגישה למאגרי המידע ולמערכות המידע, לאמצעי אבטחת המידע המוטמעים בארגון, לסיכוני אבטחת המידע הקיימים בארגון ודרכי ההתמודדות עמם ולאופן ההתמודדות עם אירועי אבטחת מידע בזמן אמת. בעלי מאגרי מידע ברמת אבטחה בינונית או גבוהה יצטרכו לכלול גם התייחסות לגיבוי המידע שברשותם, לעריכת בדיקות תקופתיות ולשימוש בהתקנים נידים בארגון.
- התקנות קובעות כי ממונה אבטחת המידע לפי חוק הגנת הפרטיות (בין אם חלה חובה חוקית למונח) ובין אם ייבחר באופן אחר, לא ימלא תפקיד אחר בארגון שעלול לגרום לו להימצא סכנה עניינים למשל, מתחילת המערכת המידע בארגון ויהיה ספוף למנכ"ל או לנושא משרה בכר אחר. עוד קובעות התקנות, כי על הממונה העניין להשית הממונה את המשיבים המדרשים כדי לציית להוראות התקנות.

מיפוי מערכות מידע, סקרי סיכונים ומבדקי חדירות

- בעלי מאגרי מידע יחויבו לערוך ולהחזיק מסמך הממפה את מערכות המידע הנוגעות לכל מאגר ומאגר (לרבות חומרה, תוכנה וציוד קצה) ואת אמצעי האבטחה החלם עליהן.
- בעלי מאגרי מידע ברמת אבטחה גבוהה יידרשו גם לערוך סקרי סיכונים ומבדקי חדירות למערכות המידע שברשותם אחת ל-18 חודשים, לדון בתוצאותיהם ולאמץ נהלים ואמצעי אבטחה בהתאם למסקנות הנוגעות מהם.

אמצעי אבטחת מידע

• בעלי מאגרי מידע יחויבו לפי התקנות להטמיע אמצעי אבטחת מידע שונים בארגון. כך למשל, יהיה על בעלי מאגרי מידע לדאוג, בין היתר, לאבטחה פיזית של המאגר, לניהול הרשאות גישה בארגון, לקביעת מנגנוני זיהוי ואימות (לרבות סיסמאות חזקות ואמצעי זיהוי חכמים), לתיעוד של אירועי אבטחה במערכות המידע, להפרדה בין מערכות המידע השונות הנוגעות למאגר ולהצפנת העברת מידע מהמאגר ברשתות ציבוריות.

• בעלי מאגר מידע ברמת אבטחה בינונית וגבוהה יחויבו לתעד את הגישה הפיזית למערכות המידע בארגון, להנהיג מנגנון קפדני של זיהוי ואימות משתמשים (לרבות מנגנוני ניתוק אוטומטיים וזיהוי באמצעים פיזיים), לתעד באופן אוטומטי את הגישה האלקטרונית למערכות המידע בארגון, ולשמור את נתוני התיעוד במשך 24 חודשים לפחות. עוד מורות התקנות כי על בעל המאגר לקבוע והלים הנוגעים לגיבוי ושחזור המידע ולבצע אחת ל-24 חודשים לפחות ביקורת פנימית או חיצונית שמטרתה לבחון את היעילות להוראות התקנות.

ניהול מורשים לגישה למאגר מידע

- התקנות מחייבות בעלי מאגרי מידע לנקוט בהליכים הולמים על מנת לוודא שעובדים שיש להם גישה למאגר מידע מתאימים לקבלת המידע המצוי בו, וזאת בשים לב לרגישות המידע. בנוסף, בעלי מאגרי מידע יחויבו לקיים הדרכות לעובדים בטרם יקבלו גישה למאגרי המידע.
- בעלי מאגרי מידע ברמת אבטחה בינונית וגבוהה יחויבו לקיים פעילות הדרכה תקופתית לעובדיהם אחת לשנה לפחות. חובות אלה תחולנה גם על עובדים המועסקים בארגון כיום ולהם גישה למאגרי המידע.



▲