

נוהל מס' 01.08.12	קובץ נהלי החברה
מהדורה מס': 1 מתאריך: 24.9.2019	פרק: משאבים ומנהל
עמוד מס': 1 מתוך 8 עמודים	פרק משנה: אבטחת מידע
שם הנוהל : אבטחת מאגר מידע	

1. כללי

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "התקנות") מפרטות את אופן יישומה של חובת אבטחת המידע המוטלת מכח חוק הגנת הפרטיות, תשמ"א - 1981 (להלן: "החוק") על בעל מאגר מידע, מנהל או מחזיק במאגר מידע. בין היתר, מחייבת תקנה 3(2) לתקנות את בעל המאגר לקבוע נוהל אבטחת מידע, שמטרתו לייצר מדיניות ארגונית להתמודדות עם סיכוני אבטחה להם חשוף המידע.

2. מטרה

מטרת נוהל זה הינה להגדיר את השיטה, האחריות והסמכות, בכל הנוגע לניהול מאובטח של מאגרי מידע בחברה על פי חוק ותקנות הגנת הפרטיות.

3. הגדרות

- 3.1. **החברה** : נתיבי ישראל-החברה הלאומית לתשתיות תחבורה בע"מ.
- 3.2. **מאגר מידע** : אוסף נתוני המידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט - אוסף לשימוש אישי שאינו למטרות עסק ולמעט אוסף הכולל רק שם, מען ודרכי התקשרות, ובלבד שלבעל האוסף אין אוסף נוסף ובו פרטים נוספים לגבי אנשים אלה הנכללים באוסף.
- 3.3. **מורשה גישה למאגר** : כל מי שמורשה לעשות שימוש במידע המצוי במאגר מידע ממוחשב של החברה.
- 3.4. **אירועי אבטחת מידע** : פעילות העלולה לגרום לפגיעה בסודיות, אמינות או זמינות המידע (לדוגמה התפשטות וירוס על עמדות קצה, אובדן או גניבה של מחשב נייד, חדירה לא מורשית למערכות המחשוב המשרתות את מאגר המידע).
- 3.5. **בעל המאגר** : החברה הינה הבעלים של מאגר המידע המצוי ברשותה.
- 3.6. **מנהל המאגר** : מנהל פעיל בחברה שבעל המאגר מינה אותו בכתב מינוי להיות אמון על המידע וליישם את תקנות הגנת הפרטיות.
- 3.7. **אירוע אבטחה חמור** : אירוע שנעשה בו שימוש במידע מן המאגר בלא הרשאה או בחריגה מהרשאה או שנעשתה פגיעה בשלמות המידע.

נוהל מס' 01.08.12	קובץ נהלי החברה
מהדורה מס': 1 מתאריך: 24.9.2019	פרק: משאבים ומנהל
עמוד מס': 2 מתוך 8 עמודים	פרק משנה: אבטחת מידע
שם הנוהל: אבטחת מאגר מידע	

4. השיטה

4.1. ניהול מסמך הגדרות מאגר

עבור כל מאגר מידע, ינוהל מסמך הגדרות המאגר. המסמך יגדיר, לכל הפחות, את הנושאים הבאים:

- 4.1.1. תיאור כללי של פעולות האיסוף והשימוש במידע.
- 4.1.2. תיאור מטרות השימוש במידע.
- 4.1.3. סוגי המידע השונים הכלולים במאגר המידע.
- 4.1.4. פרטים על העברת מאגר המידע או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה.
- 4.1.5. פעולות עיבוד מידע באמצעות מחזיק.
- 4.1.6. הסיכונים העיקריים של פגיעה באבטחת המידע, ואופן התמודדות עמם.
- 4.1.7. שמו של מנהל מאגר המידע ומחזיק המאגר.
- 4.1.8. פרטי אמצעי ההגנה הקיימים.
- 4.1.9. יש לעדכן את מסמך הגדרות המאגר, אחת לשנה, באם התקיים אחד מאלה:
 - (א) נעשה שינוי משמעותי בכל אחד מהנושאים המפורטים בסעיפים 4.1.1 עד 4.1.7.
 - (ב) נעשו שינויים טכנולוגיים רלוונטיים.
 - (ג) נעשו שינויים ארגוניים רלוונטיים.
 - (ד) אירע אירוע אבטחה המצריך עדכון של הנוהל.
- 4.1.10. אחת לשנה יש לבדוק אם לא מוחזק במאגר מידע רב מדי מזה הנדרש למטרותיו.
- 4.1.11. מסמך הגדרות המאגר ינוהל ויעודכן על ידי מנהל המאגר בסיוע של מחלקת אבטחת מידע ואגף מערכות מידע.

4.2. אבטחה פיזית

- 4.2.1. אבטחה פיזית נדרשת לתת מענה מפני פגיעה פיזית במידע ובמערכות התקשוב המשרתות את מאגר המידע.
- 4.2.2. מנהל הביטחון אחראי על אספקת והפעלת אמצעי האבטחה הפיזית, בהתאם לדרישות מנהל אבטחת מידע.
- 4.2.3. מערכות תקשוב המשרתות את המאגר יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה (חדר השרתים של החברה).
- 4.2.4. ינקטו אמצעים לבקרה ותיעוד של הכניסה והיציאה מהאתרים המכילים את מערכות המאגר.

נוהל מס' 01.08.12	קובץ נהלי החברה
מהדורה מס': 1 מתאריך: 24.9.2019	פרק: משאבים ומנהל
עמוד מס': 3 מתוך 8 עמודים	פרק משנה: אבטחת מידע
שם הנוהל: אבטחת מאגר מידע	

4.3. הרשאות גישה

- 4.3.1. הרשאות גישה למאגר המידע ולמערכות המאגר יקבעו בהתאם להגדרות התפקיד. לכל תפקיד תינתן גישה, אך ורק, במידה הנדרשת לביצוע התפקיד בלבד.
- 4.3.2. מנהל המאגר ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם ושל בעלי ההרשאות הממלאים תפקידים אלה.
- 4.3.3. מידור המידע והרשאות שימוש במערכות המאגר יבוצע על פי סעיף 11 בנוהל מדיניות אבטחת מידע והסייבר.

4.4. הוראות למורשי הגישה למאגר המידע

- 4.4.1. ככלל, חל איסור על הוצאה/מסירה של מידע ממערכות המאגר שלא על פי הגדרות מטרות המאגר, המפורטות במסמך הגדרות המאגר.
- היה ונדרש, יש לקבל מראש אישור ממנהל המאגר בדבר הוצאה/מסירה של מידע לגורם חיצוני ולעדכן, במידת הצורך, את מסמכי המאגר.
- 4.4.2. חובת מורשי הגישה לעדכן את מנהל המאגר ואת מחלקת אבטחת המידע בכל חשד לאירוע אבטחה שבעקבותיו נחשף או נפגע מידע שנכלל במאגר.

4.5. סיכונים להם חשוף המידע במאגר

- קיימים מספר סיכונים למידע במאגר, העלולים לחשוף את המאגר לפגיעה בזמינות, אמינות וחסינות המידע.
- סיכונים אלו יכולים להתרחש ע"י תוקף חיצוני אשר מנסה לחדור את מערכות החברה, וכן ע"י עובד החברה (בזדון או בלא כוונת תחילה).
- ההתמודדות עם הסיכונים תבוצע ע"י מימוש בקורות גישה ומידור הרשאות על בסיס Least Privilege, הגנה בשכבות, חסימת התקנים חיצוניים, גיבוי.

4.6. מסמך מבנה המאגר ומערכות מחשוב

- 4.6.1. לכל מאגר מידע יתלווה מסמך שיפרט את מבנה המאגר וכן רשימת מצאי מעודכנת של מערכות המאגר ובכלל זה יפרט המסמך:
- 4.6.2. תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע.
- 4.6.3. מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו.
- 4.6.4. תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן.
- 4.6.5. תרשים הרשת שפועל בה המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של רכיבים אלה.

נוהל מס' 01.08.12	קובץ נהלי החברה
מהדורה מס': 1 מתאריך: 24.9.2019	פרק: משאבים ומנהל
עמוד מס': 4 מתוך 8 עמודים	פרק משנה: אבטחת מידע
שם הנוהל : אבטחת מאגר מידע	

4.6.6. הסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת של בעל מאגר המידע ואופן הטיפול בהם.

4.6.7. תאריך העדכון האחרון של המסמך ושל רשימת המצאי.

4.7. התקנים ניידים

ככלל, חל איסור לחבר התקנים ניידים למערכות המקושרות למאגר המידע. היה ונדרש לחבר התקן נייד, יש לפעול על פי נוהל אבטחת רכיבים נתיקים.

4.8. אירועי אבטחת מידע

4.8.1. מנהל המאגר (בעזרת אגף מערכות מידע) אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות, סודיות וזמינות המידע או לשימוש בו ללא הרשאה או לחריגה מהרשאה.

4.8.2. התמודדות ואופן הטיפול באירועי אבטחת מידע יבוצעו לפי נוהל טיפול באירוע אבטחת מידע.

4.8.3. בעת אירוע אבטחה חמור מנהל המאגר יודיע על כך לרשם מאגרי המידע באופן מיידי, וכן ידווח על הצעדים שננקטו בעקבות האירוע.

4.8.4. אחת לשנה יקיים מנהל המאגר (בעזרת מחלקת אבטחת המידע) דיון בנושא אירועי אבטחת מידע, בהתאם לסיווג אבטחת מאגר המידע, ובמידה והיה אירוע אבטחה ויבחן את הצורך בעדכונו של נוהל זה.

4.9. זיהוי ואימות

מנהל המאגר (באמצעות אגף מערכות מידע) ינקוט אמצעים מקובלים בנסיבות העניין ובהתאם לאופי המאגר וטיבו, כדי לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך ולפי רשימת ההרשאות התקפות שאושרו בוועדת ההרשאות.

הליך הזיהוי יכלול:

(א) שם משתמש.

(ב) סיסמא

(ג) זיהוי משתמש

(ד) תוקף הסיסמה יפוג לאחר חודשים.

(ה) המשתמש ינעל לאחר ניסיונות חיבור כושלים.

נוהל מס' 01.08.12	קובץ נהלי החברה
מהדורה מס': 1 מתאריך: 24.9.2019	פרק: משאבים ומנהל
עמוד מס': 5 מתוך 8 עמודים	פרק משנה: אבטחת מידע
שם הנוהל : אבטחת מאגר מידע	

- (ו) יבוצע ניתוק אוטומטי לאחר פרק זמן של אי-פעילות, על פי הגדרות פרקי הזמן המוגדרים במערכות המשרתות את המאגר.
- (ז) הטיפול בתקלות הקשורות באימות הזהות ייעשה על פי נהלי העבודה בחברה.
- (ח) יבוטלו ההרשאות של עובד שסיים את תפקידו.
- (ט) הליך מתן הרשאות וניהול זהויות יבוצע בכפוף לנוהל מדיניות ניהול זהויות וטיפול בהרשאות.

4.10. בקרה ותיעוד גישה

- 4.10.1 ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר כאשר הליך התיעוד יכלול נתונים אלו:
- (א)
- (ב)
- (ג)
- (ד)
- (ה)
- 4.10.2 מנהל המאגר (בעזרת מנהל אבטחת מידע) יקבע נוהל בדיקה שגרתי של נתוני התיעוד ויערוך דוח של הבעיות שהתגלו וצעדים שנקטו לפתרון.
- 4.10.3 נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות או שניתן יהיה לשחזרם עבור תקופה זו.
- 4.10.4 מנהל המאגר יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.

4.11. ביקורות תקופתיות

מנהל המאגר (בעזרת מחלקת אבטחת המידע) אחראי לכך שתיערך, אחת ל- 24 חודשים לפחות, ביקורת פנימית או חיצונית על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע, בכדי לוודא את קיומן של תקנות הגנת הפרטיות. מנהל המאגר, בתאום עם אגף מערכות מידע, ידון בדוחות הביקורת שיועברו לעיונו ע"י מחלקת אבטחת מידע ויבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה.

נוהל מס' 01.08.12	קובץ נהלי החברה
מהדורה מס': 1 מתאריך: 24.9.2019	פרק: משאבים ומנהל
עמוד מס': 6 מתוך 8 עמודים	פרק משנה: אבטחת מידע
שם הנוהל: אבטחת מאגר מידע	

4.12. גיבוי המידע

מנהל המאגר (בעזרת אגף מערכות המידע) יבחן את הנהלים והמדיניות של החברה בנוגע לגיבוי כולל של החומרים במערכות החברה. ככל שיימצא לנכון, יקבע נהלים ייעודיים למידע בהתאם לרמת האבטחה שחלה עליו, במאגר המידע שבאחריותו. הליכי שחזור המידע יתועדו ויכילו את זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר. המידע ישמר לכל הפחות, למשך של 24 חודשים.

4.13. פיתוח ותחזוקה של מערכות המאגר

הליך הפיתוח ותחזוקה של מערכות המשרתות את המאגר יבוצעו על פי הנחיות ונהלים, ככל שקיימים בחברה. גישת מפתחים למערכות המשרתות את המאגר בסביבות הייצור תצומצם למינימום האפשרי בכדי למנוע פגיעה בזמינות, שלמות וחסינות המידע.

4.14. עדכון הנוהל

אחת לשנה ידון מנהל המאגר, יחד עם מנהל מחלקת אבטחת המידע, בנוגע לעדכון נהל זה, במידה ונעשו שינויים מהותיים במערכות המאגר או בתהליכי עיבוד המידע וכן אם נודע על סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר.

5. סמכות ואחריות

5.1. אחריות מנהל המאגר

מנהל מאגר מידע (ביחד עם בעל מאגר המידע) אחראי על קביעת מדיניות אבטחת מידע על מנת להבטיח קיום הוראות החוק והתקנות בתחומים הבאים:

- 5.1.1. רישום מאגר המידע אצל רשם מאגרי המידע.
- 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 המצויים בחוק (כגון, חסיון כלשהו, מידע רפואי).
- 5.1.4. אבטחת המידע, תוך שימת לב לנושאים הבאים:
 - (א) הגנה פיזית על המידע.
 - (ב) מדיניות הגישה למידע.
 - (ג) אישור או מניעת העברת וחשיפת המידע לגורם חוץ.
 - (ד) ביקורות תקופתיות.
 - (ה) מדיניות הגיבויים ושמירה של המידע.
 - (ו) הדרכות לעובדים חדשים וכאלו שיש להם גישה למידע המצוי במאגר.

נוהל מס' 01.08.12	קובץ נהלי החברה
מהדורה מס': 1 מתאריך: 24.9.2019	פרק: משאבים ומנהל
עמוד מס': 7 מתוך 8 עמודים	פרק משנה: אבטחת מידע
שם הנוהל : אבטחת מאגר מידע	

5.2. אחריות אגף מערכות מידע

באחריות אגף מערכות מידע לתחזק את מערכות 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 תשתיות מיזוג, אויר וכיבוי אש מתאימים.
- 5.2.2. הגישה הפיזית למערכות מוגבלת למורשים בלבד כל גורם לא מורשה יקבל ליווי בעת ביצוע העבודות.
- 5.2.3. המערכות מוגדרות ומתוחזקות בהתאם לנוהל זה.
- 5.2.4. מבוצע גיבוי למידע ולמערכות אבטחת המידע המשרתות את המאגר, בהתאם למדיניות הנקבעת בשיתוף מנהל המאגר תבוצע בדיקה תקופתית של הגיבויים ע"י שחזורים יזומים, כדי לוודא שהמידע אמין וניתן לשחזור בעת הצורך.
- 5.2.5. ננקטים אמצעי אבטחה סבירים כגון חומת אש, IPS, אנטי וירוס, תיעוד גישה למערכות המאגר, תיעוד גישה פיזית שימנעו חדירה מכוונת או מקרית למערכות

5.3. אחריות מחלקת אבטחת מידע



מחלקת אבטחת מידע תסייע למנהל המאגר לעמוד בכל החובות החלות עליו מתוקף תקנות אבטחת המידע ותתריע בפניו מיד אם מתגלה לה ליקוי באבטחת המידע. באחריות מנהל מחלקת אבטחת המידע לבצע פיקוח ובקרה על יישום נוהל זה.

6. מסמכים ישימים


- 6.1. מדיניות אבטחת המידע.
- 6.2. מדיניות ניהול זהויות וטיפול בהרשאות.
- 6.3. נוהל שימוש ואבטחת רכיבים נתיקים.
- 6.4. תפיסת הפעלה אבטחת מידע.
- 6.5. נוהל טיפול באירוע אבטחת מידע וסייבר.

נוהל מס' 01.08.12	קובץ נהלי החברה
מהדורה מס': 1 מתאריך: 24.9.2019	פרק: משאבים ומנהל
עמוד מס': 8 מתוך 8 עמודים	פרק משנה: אבטחת מידע
שם הנוהל : אבטחת מאגר מידע	

נבדק על ידי:

תפקיד	שם ומשמחה	תאריך	חתימה
מנהלת אגף ארגון ושיטות	טלי אבידן	24.9.19	
מנהל מחלקת אבטחת מידע	צחי לביא	25.9.2019	

אושר על ידי:

תפקיד	שם ומשמחה	תאריך	חתימה
יו"ר וועדת החיגוי לאבטחת מידע סמנכ"ל משאבים ומנהל	אריה דהן	2/10/2019	

טבלת מהדורות:

מהדורה	תאריך עדכון	כותב הנוהל	גורם אחראי	מהות השינוי
1.0	24.9.2019	צחי לביא וטלי אבידן	אריה דהן	מהדורת בסיס