נוהל אבטחת מידע

בהתאם לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, סעיף 2 א:

- הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר כאמור בתקנה 6
  - שרתים בחווה המאובטחת של אמזון שמאבטחת בצורה פיזית את חוותיה.
  - הרשאות גישה למאגר המידע ולמערכות המאגר בהתאם לתקנה 8
  - העברת הדרכות לבעלי הרשאות בנושא החובות לפי החוק ותקנות אלה ומסירת מידע אודות חובותיהם לפי החוק ונוהל האבטחה.
  - מתן שם משתמש וסיסמה יעודיים לגישה למאגר באמצעות מערכת ביניים המאפשרת שינוי חלקים רלוונטיים בלבד, מתעדת את הנעשה ומספקת 4 מנגנוני הגנה עיקריים
- מחיקה מיידית של המשתמש

♣ שינוי סיסמה למשתמש

♣ חסימה טוטאלית של כלל המשתמשים במערכת בלחיצת כפתור

♣ הצפנה של מידע רגיש כדוגמת סיסמאות (גם במקרה הכי גרוע לא ניתן להבין ע"פ הנתונים הגולמיים במאגר את המידע הרגיש)

♣ תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך:
  - גישה ישירה לשרת דרך פורטים בודדים הידועים רק לבעל המאגר ואנשיו.
  - חסימת טואטלית של הגישה למערכת למעט כתובות IP בודדים שידועים מראש שרק מהם ניתן לגשת
  - איסוף נתונים כולל על המשתמש בכל פעולה שהוא מבצע (סוג המכשיר, מערכת ההפעלה והדפדפן שבה משתמש, IP ממנו מבוצעת הפעולה ותיעוד הפעולה עצמה בדוח נפרד)
  - וידוא יומיומי של תעודות אבטחה (SSL) בתוקף של כל הכתובות הנוגעות במאגר וחידוש מיידי ברגע שפג תוקף
  - החתמה על מסמך סודיות של כל הנוגע במערכת
  - שמירת גיבויים יומיים, שבועיים וחודשיים ואפשרות לשחזר.
  - אופן זיהוי מקבל המידע נעשה על הטלפון שלו בלבד ומחייב הזנת קוד אימות שנשלח במסרון בעת מילוי הפרטים, כלומר אופן זיהוי מקבל המידע נעשה על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה.
  - הגדרת SESSION TIME OUT לאחר פרק זמן של אי פעילות, המחייב זיהוי מחדש של מזין המידע.
  - חומת אש.
  - הוראות למורשי הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר
  - נגיעה במאגר אך ורק דרך מערכת ביניים ומעקב רציף ומילוי ההוראות על המסך.
  - הסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה הנובעים ממבנה מערכות המאגר כמפורט בתקנה 5
    1. מחיקת מידע
    2. שינוי מידע בכל צורה שהיא
    3. שימוש במידע לצורך העברתו לגורם שאינו מורשה

♣ אופן קביעת סיכונים אלה

- הסיכונים נקבעו ע"י מפתחי המערכת שמכירים אותה על בוריה

♣ אופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות המאגר
- הצפנה ושיטות חסימה מפורטות בתיאור האמצעים מעלה.
- מחיקת מידע שחזור מידע
- שינוי מידע שחזור מידע
- העברת מידע לגורם שאינו מורשה טיפול משפטי + חסימה (במידה האפשר) לאפשרות משלוח

♣ אופן התמודדות עם אירועי אבטחת מידע כאמור בתקנה 11, לפי חומרת האירוע ומידת רגישות המידע
- פעילות באמצעים שפורטו מעלה בהתאם לאירוע האבטחה.

♣ הוראות לעניין ניהול של התקנים ניידים ושימוש בהם כאמור בתקנה 12
- את ההתקנה רשאי לבצע כל גורם מוסמך מטעם מנהל המאגר בהתאם להנחיות העדכניות שדורשת המערכת ובהתאם לכל התקנות הנ"ל

♣ אמצעי הזיהוי והאימות לגישה למאגר ולמערכות המאגר, בהתאם לתקנה 9
- שם משתמש וסיסמה כאמצעי זיהוי במקרה של מזין תוכן
- וי סימון להוכחה שהמשתמש אינו רובוט ברגע ההתחברות

- חוזק הסיסמה– ללא הגבלה. אחת לחצי שנה תתבצע החלפת הסיסמה.
- מספר ניסיונות כושלים –3. לאחר מכן תתבצע נעילה של המשתמש שיצטרך לפנות לתמיכה כדי לשחרר את נעילתו.

- טלפון והזנת קוד אימות שנשלח לאותו הטלפון בעת מילוי הפרטים במקרה של מקבל מידע פוטנציאלי
  - חוזק קוד האימות – 4 ספרות רנדומליות
  - מספר ניסיונות כושלים – ללא הגבלה אך הקוד משתנה בכל ניסיון כושל.

- אופן הבקרה על השימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות המאגר כאמור בתקנה 10
  - פירוט בסעיף אמצעי ההגנה שמופיע מעלה

- הוראות לעניין עריכת ביקורות תקופתיות לווידוא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה כאמור בתקנה 16
  - אחת לכל תקופה יהיה רשאי מנהל המאגר או מי מטעמו לבצע ביקורת פתע על הנוהל והתוכנית לעמידה בדרישות תקנות אלה

- הוראות לעניין גיבוי הנתונים האמורים בתקנה 18
  - פירוט בסעיף אמצעי ההגנה שמופיע מעלה

- הוראות לעניין אופן ביצוע פעולות פיתוח במאגר ותיעודן, ובכלל זה אופן הגישה של אנשי הפיתוח לנתונים במאגר.
  - נכון לשלב זה עדכוני תוכנה יבוצעו ע"י מנהל המאגר או מי מטעמו ויוטמעו ע"י מנהל המאגר בלבד.

- <u>תכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה</u>
  - מנגנון חידוש תעודות אבטחה אוטומטי AutoSSL
  - מנגנון גיבוי אוטומטי לפי הנוהל
  - מסך יעודי ליצירת משתמש שאמור לקבל גישה למאגר עם צ'קליסט של הנוהל שלא מאפשר התקדמות ללא וידוא הפעולות הנדרשות.
  - אישור מסמך הסודיות ע"י עורך דין חיצוני וטיפול משפטי במידת הצורך
  - אחת לשנה נבצע שינויים במסמך זה במידת הצורך
  - לפחות אחת ל-18 חודשים או במקרה של שינוי ארכיטקטורה נערוך גם סקר סיכונים מחודש
  - לפחות אחת לשנתיים נקיים פעילות הדרכה תקופתית לבעלי הרשאות, בדבר מסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה
  - ננהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה
  - מנגנון המחייב שינוי סיסמה אחת לחצי שנה למזיני התוכן
  - בקרה ותיעוד גישה וניסיונות התחברות (זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.) נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.
  - ברגע שמזין תוכן שכח סיסמה, באפשרותו לשלוח מייל על מנת לקבל סיסמה חדשה
  - לפחות אחת לשנה תתבצע בדיקה שגרתית של נתוני התיעוד של מנגנון הבקרה, ונערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.
  - נערוך תיעוד מלא של אירועי האבטחה במקביל לפעילות המערכת
  - במקרה של אירוע אבטחה חמור ניידע גם את רשם הרשות הלאומית להגנת הסייבר.
  - במסגרת תיעוד אירועי אבטחה כאמור בתקנה 11 ,יתועדו גם הליכי שחזור המידע, ובכלל זה - זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר.
  - במקרה של העסקה מטעם מנהל המאגר להגביל את הפרטים הבאים:
  - המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות.
  - מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן.
  - סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות.
  - משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע.
  - אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע.
  - חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם כאמור בפסקת משנה.

הסכם התקשרות

- התיר בעל מאגר מידע לגורם החיצוני לתת את השירות באמצעות גורם נוסף - חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו.
- חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחה.
- אחת ל–24 חודשים לפחות, נערוך ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע שאינו ממונה האבטחה של המאגר, כדי לוודא את עמידתו בהוראות תקנות אלה.

- <u>מיפוי מערכות המאגר</u>
  - תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע
  - שרת לינוקס בחוות השרתים המאובטחת של אמזון
  - קבוצת Network Security עם כללים מחמירים האפשרי גישה בפורטים בודדים הידועים רק למנהל המאגר או מי מטעמו.
  - חסימה טוטאלית למערכת למעט IP בודדים שמוגדרים וידועים מראש
  - גיבויים
  - מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו
  - CentOS
  - WHM
  - SSH
  - Kernel Care
  - אנטיוירוס ImunifyAV
  - תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן
  - phpMyAdmin
  - cPanel
  - רכיבי תוכנה בפיתוח אישי
  - תרשים הרשת שפועל בה המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של רכיבים אלה
  - שרת לינוקס בחוות השרתים המאובטחת של אמזון
  - תוכנת עזר למשלוח מסרים בווצאפ על מכשירי המועצה (קשר אינטרנטי מרוחק עם קוד הגנה יעודי למועצה)
  - תאריך העדכון האחרון של המסמך ושל רשימת המצאי.
  - 18/01/2021

- <u>ביצוע סקר סיכונים</u>
  - פריצה פיזית לחוות של אמזון סיכוי אפסי
  - כניסה לא מורשית ו/או שימוש לא מורשה של אנשי אמזון בעצמם סיכוי אפסי
  - פריצה וירטואלית למערכות התוכנה סיכוי מזערי אם מנגנוני הגנה שמספקות: אמזון ו-WHM
  - פריצה לרכיבי התוכנה המנהלת את מערכת (גישה למשלוח תכנים) סיכוי אפסי עם אפשרות למחוק את המשתמש, לשחזר את המידע ששינה או מחק, לחסום גישה כוללת לכלל המשתמשים, לחסום את אפשרות משלוח המסרים (במידת האפשר).
  - התחזות למקבל מידע לא אמיתי ע"י פרטים של משתמש אחר סיכוי אפסי מכיוון שדרושה גישה פיזית למכשיר הטלפון ממנו נרשם מקבל המידע הפוטנציאלי + בשינוי פרטים/מענה על סקר/אישור הגעה לאירוע נדרשות 4 הספרות הסודיות של מזהה המשתמש (מיוצר ע"י UUID) בתוספת המספר הרץ של אותו המשתמש
  - גניבה של קוד התוכנה סיכוי מזערי עם אפשרות לשנות את מילת המפתח של המנגנון המצפין (במקרה כזה הוא אולי יצליח להפעיל את המערכת במקביל אך כל הנתונים המוצפנים במאגר לא יהיו תקפים יותר.) יותר מכך, סיסמאות הכניסה מוצפנים באופן חד כיווני כך שגם אם לא נספיק לשנות את מילת המפתח לא ניתן לדעת את הסיסמאות. יתר על כן גם במצב של עבודה שוטפת אין אפילו למנהל המאגר את היכולת והאפשרות לדעת סיסמאות
  - גניבה של המאגר סיכוי שואף לאפס מכיוון שכרוך בעקיפה של כל מנגנוני ההגנה המפורטים מעלה. במקרה כזה תיתכן השבתה זמנית מכוונת מצידינו של המערכת וטיפול משפטי.

- <u>מסמך הגדרות המאגר</u>
  - <u>תיאור כללי של פעולות האיסוף והשימוש במידע:</u>
  - המאגר אוסף ממקבלי המידע הפוטנציאליים (בעיקר תושבים)

♣ פרטים אישיים

הסכם התקשרות

- פרטי התקשרות
- העדפות אישיות
- הכלים בהם נעשה שימוש (סוג המכשיר, מערכת ההפעלה, דפדפן)
- היסטוריית פעילות במערכת
  - השימוש במידע הינו העברת מסרים רלוונטיים באמצעים הרצויים בהתאם להעדפות מקבלי המידע
  - תיאור מטרות השימוש במידע
  - העברת מסרים רלוונטיים כגון
- הזמנה לאירוע שעתיד להתקיים
- ידיעה לתושבי ומתגוררי המקום
- סיקור אירועי עבר רלוונטיים
  - באמצעים הרצויים (וואטסאפ, מייל, סמס). האמצעים עשויים להשתנות.
  - בהתאם להעדפות מקבלי המידע
- תחומי עניין (חינוך, ספורט, בריאות, טיולים וסיורים, איכות סביבה, אמנות ויצירה, הרחבת אופקים, לימודים והעשרה, מסיבות ואירועים, תיאטרון ומשחק, מחשבים ואינטרנט, טכנולוגיה ומדע, ריקוד ומחול, מוסיקה, דת ורוחניות, החלטות מועצה, יוזמות עירוניות, חדשות בישוב). התחומים עשויים להשתנות.

- שכבות גיל הגיל הרך (1-5), ילדים (6-11), נוער (12-18 , צעירים (19-35), מבוגרים (36-64), ותיקים (65+), כל הגילאים). שכבות הגיל עשויות להשתנות.

- תזמון: אזורים גאוגרפיים – מרכז העיר, מערב העיר, מזרח העיר

- סוגי המידע השונים הכלולים במאגר המידע (הפרטים עשויים להשתנות):
  - קהלי מטרה (שכבות הגילאים שמפורטים מעלה)
  - סוגי דפדפנים ומערכות הפעלה הקיימות בשוק
  - המועצות המשתמשות בשירות
  - מיילים להתראות
  - ידיעות, סיקורים, הזמנות לאירוע וכל הפרסומים שמפרסמים כלל הרשויות
  - תחומי העניין של קהלי המטרה (מפורט מעלה)
  - תיעוד כל הקורה במערכת
  - תור למשלוח עכשווי ועתידי של מזיני התוכן מטעם המועצות במערכת
  - היסטוריית משלוח ותוצאת השליחה למשתמשים
  - הגדרות מערכת
  - משתמשים (מקבלי מידע, מזיני מידע, מנהלים)
  - פרטים על העברת מאגר המידע, או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה, מטרת ההעברה, ארץ היעד, אופן ההעברה וזהות הנעבר
  - המידע מאוחסן בחוות השרתים של חברת אמזון שנמצאת באזור בלגיה (מערב אירופה). המידע לא מועבר אלא מאוחסן ומתופעל בשרת בחווה. הנ"ל נמצא בחו"ל למטרות ביצועים משופרים 703\1\86-1