מדינת ישראל
משרד החינוך
מנהל תקשוב טכנולוגיה ומערכות מידע

הנחיות אבטחת מידע למתי״א

יולי 2019

מערכת החינוך מטפלת בכמויות רבות של מידע אישי, פרטי ורגיש של אוכלוסיות רבות בישראל. כאשר מדובר בחינוך המיוחד עובדה זו מקבלת משנה תוקף. לצורך התמיכה, הסיוע והטיפול שאנו מספקים לאוכלוסייה, אנו מקבלים גישה לפינות הרגישות והפרטיות ביותר. הנזק העלול להיגרם מחשיפה של מידע פרטי זה הוא רב, ועלינו מוטלת האחריות לשמור עליו מכל משמר. לצורך כך, יש להתנהל במתי״א ברמת אבטחת מידע גבוהה ביותר, תוך מודעות של כלל הגורמים המעורבים לנושא.

1. **הגדרות**

א. **מידע מוגן**: נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו. לדוגמה: קובץ המכיל רשימה עם מספרי זהות, פרטי קשר, מידע על תלמידים ועובדים (כגון רשימת תלמידים/עובדי הוראה, תמונה, חוות דעת, אבחון, ציונים, נתונים כספיים ועוד).

ב. **מאגר מידע:** אוסף נתוני מידע המוחזק באמצעי מגנטי או אופטי (ובכלל זה מחשב) או פלט מודפס, ומיועד לעיבוד ממוחשב.

ג. **נזק למידע**: פגיעה בסודיות, בשלמות ובזמינות המידע בבעלותו של משרד החינוך, ו/או פגיעה בפרטיות של משתמשים.

1. **הנחיות**

1.1 האחריות לאבטחת המידע במתי״א היא של מנהל/ת המתי״א. על מנהל/ת המתי״א לוודא כי ההנחיות המופיעות במסמך זה מיושמות בפועל.

1.2 **ניהול גישה והרשאות למערכות מידע המכילות מידע מוגן**

1.2.1 יש לוודא כי הרשאות הגישה למידע או השימוש במערכות יינתנו בהתאם לצורך של המשתמש לשימוש במידע.

1.2.2 לכל בעל תפקיד יינתנו הרשאות גישה למידע מוגן, אך ורק בהתאם לצורך שלה/ו לביצוע התפקיד. יש לאסור שימוש בהרשאות גישה של משתמשים/בעלי תפקיד אחרים.

1.2.3 במקרה של עזיבת בעל תפקיד יש לוודא כי הרשאות הגישה שלה/ו למערכות המכילות מידע מוגן יבוטלו.

1.2.4 יש לוודא כי צוות המתי״א מודע ושומר על כללים לשמירת וניהול סיסמאות:

א. סיסמאות הן אישיות ואין למוסרן לאחרים

ב. יש לבחור סיסמאות מורכבות עם אורך מינימלי של 8 תווים.

ג. אין לבחור סיסמאות זהות לסיסמאות בהן נעשה שימוש בחשבונות אישיים אחרים.

1.3 **שימוש במערכות טכנולוגיות**

1.3.1 במידה ונעשה שימוש במערכות טכנולוגיות חיצוניות לניהול וטיפול בצרכי המתי״א, כגון שיבוץ, ניהול מלאי וכדומה, יש לעשות שימוש אך ורק בשירותים טכנולוגיים אותם מספק משרד החינוך או במוצרים טכנולוגיים שעברו בדיקות אבטחת מידע וקיבלו אישור של משרד החינוך;

1.3.2 רשימת המוצרים הטכנולוגיים המאושרים מופיעה ב״קטלוג החינוכי״ בקישור הבא: הקטלוג החינוכי. במידה וספק מעוניין לקבל אישור למערכת טכנולוגית יש להפנותו לדף המידע: מידע לספקים טכנולוגיים.

1.3.3 התחברות למערכות מידע המכילות מידע מוגן תבוצע באמצעות הזדהות חזקה (2 factor authentication).

1.4 **ניהול והגנת מחשבי המתי"א**

1.4.1 יש לוודא כי כלל המחשבים מוגנים בסיסמת כניסה.

1.4.2 יש לוודא כי על כל המחשבים במתי"א מותקנת מערכת הפעלה עדכנית שנתמכת על ידי היצרן. כיום מומלץ לעשות שימוש בגירסה האחרונה של Windows 10.

1.4.3 יש לוודא כי לכלל התוכנות המותקנות על מחשבי המתי"א ובכלל זה מערכת ההפעלה, רישיון חוקי תקף.

1.4.4 יש לוודא כי מערכת ההפעלה נתמכת על ידי היצרן ומתעדכנת באופן קבוע בעדכוני אבטחת מידע של היצרן. לקבלת רישיון למערכות הפעלה Windows ללא עלות יש ליצור קשר עם מוקד חותם: www.scool.co.il/ness, ובטלפון: 09-8922923.

1.4.5 יש לוודא כי תוכנה להגנה מפני נוזקות (כגון אנטי וירוס) מותקנת על כל המחשבים והשרתים במתי"א. על תוכנות אלה להתעדכן באופן שוטף ולבצע סריקה יומית לגילוי וניקוי נוזקות. במידה ומערכת ההפעלה היא Windows 10 ניתן לעשות שימוש באנטי וירוס המובנה (Defender) אך יש לוודא כי הוא מופעל באופן תקין, מתעדכן ומבצע סריקות באופן שוטף.

1.4.6 אין לאפשר למשתמשים במחשבי המתי"א התקנת תוכנות באופן עצמאי על המחשבים בשל החשש מנוזקות (כגון וירוסים).

1.4.7 במידה ונעשה שימוש במחשבים ניידים, יש לוודא נקיטת הפעולות הבאות:

א. המחשב הנייד מוגן בסיסמת כניסה.

ב. אנטי וירוס מותקן על המחשב, מבצע סריקה יומית ומתעדכן באופן שוטף.

ג. מערכת ההפעלה מתעדכנת באופן שוטף בעדכוני אבטחת מידע.

ד. לא נשמר או מגובה על המחשב מידע אישי ורגיש. במידה ונשמר מידע מוגן על המחשב יש לוודא כי נמחק לאחר סיום השימוש בו.

ה. יש לוודא כי הדיסק הקשיח במחשבים הניידים מוצפן (למשל על ידי תוכנת Bitlocker הקיימת במערכת ההפעלה Windows 10). זאת על מנת שבמידה והמחשב נגנב/אובד משתמשים זרים לא יוכלו לגשת למידע.

1.4.8 במידה ונעשה שימוש במערכות לניהול תצורה של עמדות קצה (כגון Deep Freeze, Radix), יש לוודא כי מערכות אלו מוגדרות באופן שמאפשר עדכוני אבטחת מידע של מערכת ההפעלה באופן שוטף, עדכון שוטף של תוכנת האנטי וירוס.
חשוב! תוכנות אלו אינן "תוכנות הגנה" ואינן תחליף להתקנת מוצר להגנה מפני נוזקות על המחשב.

1.5 **הגנות רשת**

להלן פירוט הגנות הרשת המינימליות שיש ליישם במתי"א:

1.5.1 על כלל מערכות המחשב במתי"א להימצא מאחורי "חומת אש" (Firewall) היקפית אשר מנוהלת ומתוחזקת באופן שוטף, וכי החוקים בה מאפשרים גישה מינימלית למערכות המתי"א, בהתאם לצרכיו.

1.5.2 יש לוודא שארונות התקשורת במתי"א נעולים.

1.5.3 אין לבצע חיבורים לא מורשים ("פיראטיים") לציוד התקשורת במתי"א ללא אישור.

1.5.4 במתי"א בו קיימת רשת אלחוטית Wi-Fi יש להגדיר את הגישה אליה בסיסמה. את הסיסמא יש לשנות אחת לשנה.

1.6 **שימוש בטוח בדואר אלקטרוני**

לצרכי עבודת המתי"א יש לעשות שימוש אך ורק בדוא"ל ארגוני מאובטח ולא בחשבונות דוא"ל פרטיים. דוא"ל ארגוני הוא דוא"ל שמספק משרד החינוך כגון "יונת דואר" או חשבון דוא"ל של סביבת ענן לימודית בה עושה המתי"א שימוש, כגון Office 365 for Education.

1.7 **שמירה והעברת מידע מוגן**

1.7.1 מידע מוגן ניתן לשמור במקומות הבאים:

א. מערכות משרד החינוך

ב. מוצרים חינוכיים טכנולוגיים מאושרים על ידי משרד החינוך עמם יש למוסד החינוכי התקשרות.

ג. בשרתי המתי"א.

ד. סביבות ענן מאושרות כגון Office 365 Education.

1.7.2 אין לשמור מידע מוגן ב:

א. מחשבים פרטיים (כגון מחשבים ביתיים עליהם מתבצעת עבודה)

ב. התקנים ניידים כגון (Disk on Key). במידה ונעשה שימוש בהתקן נייד יש לוודא כי הוא מוצפן.

ג. חשבונות ענן פרטיים.

1.7.3 העברה אלקטרונית של מידע מוגן צריכה להתבצע באופן מאובטח – על ידי הצפנת המידע ושימוש בכספת אלקטרונית של משרד החינוך.
בהתאם לתקנות חוק הגנת הפרטיות חל איסור להעביר מידע וקבצים המכילים מידע על התלמידים דרך הדואר האלקטרוני ללא הגנה מספקת.
במידה ובכל נעשה שימוש בדוא"ל להעברת המידע יש להגן על קבצים שמועברים בהתאם להנחיות הבאות:

א. **לפני השליחה - יש לוודא שהגורם המקבל מורשה לטפל במידע הנשלח.**

ב. הגנה על הקובץ באמצעות סיסמא (מצורף הסבר בתחתית המסמך).

ג. הסיסמא צריכה להיות מינימום 10 תווים הכוללים אות גדולה, אות קטנה ומספר.

ד. יש לוודא את תקינות כתובת הדואר האלקטרוני של הנמען.

ה. שליחת הסיסמא במייל נפרד בדואר אלקטרוני, יש לוודא את תקינות כתובת הדואר האלקטרוני של הנמען.

1.8 **סינון גלישה**

יש לוודא כי הגישה מהמתי"א לרשת האינטרנט נעשית תמיד באמצעות מנגנוני סינון גלישה לחסימת תכנים שאינם ראויים ואתרי אינטרנט זדוניים

1.9 **גיבויים**

1.9.1 יש לוודא כי למידע במתי"א נעשה גיבוי באופן קבוע למקרה שבו תהיה פגיעה במידע או במערכות המחשוב, וזאת על מנת לחזור לפעילות שוטפת קלה ומהירה.

1.9.2 מערכת הגיבויים תהיה נפרדת ממערכות המחשוב ותמוקם פיזית באזור נפרד ומאובטח.

1.10 **טיפול במידע מודפס**

1.10.1 יש לוודא כי כלל המסמכים במתי"א המכילים מידע מוגן יאוחסנו בחדרים ייעודיים מתויקים בארונות נעולים.

1.10.2 יש לוודא כי מסמכים המכילים מידע מוגן יושמדו על ידי גריסה ולא יושלכו לפח.

1.10.3 באזורי קבלת קהל לא יונח על גבי שולחנות מידע מוגן.

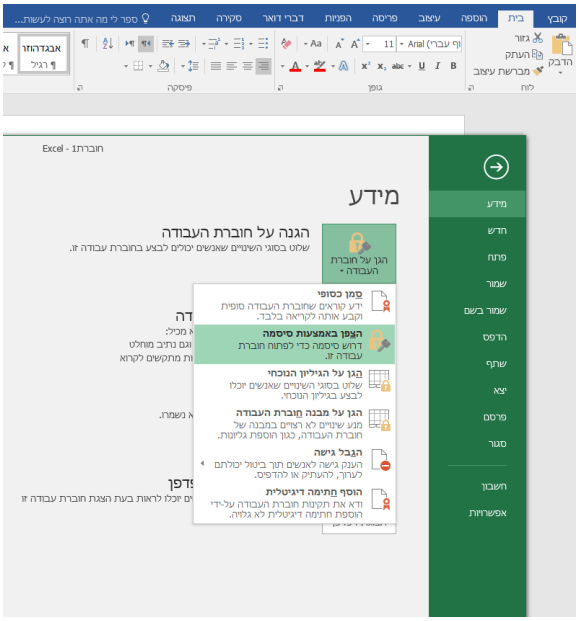
1.11 **טיפול באירועי אבטחת מידע**

בעת אירוע אבטחת מידע לזמן חשיבות רבה. ככל שמשך הטיפול באירוע יקטן, כך ניתן יהיה לצמצם את הנזק הפוטנציאלי מהאירוע. אם עולה חשד לאירוע אבטחת מידע (כגון פגיעה בפרטיות תלמידים, נוזקה על מחשב או מחשבים במתי"א, שימוש במחשבים לצורך גרימת גניבת מידע ו/או גרימה לנזק, גניבת זהות, דליפת מידע אישי לרשת האינטרנט וכדומה), יש לדווח עליו ל**יחידת ההגנה בסייבר למגזר החינוך בדוא"ל: school_security@education.gov.il. טלפון: 03-9298737.**

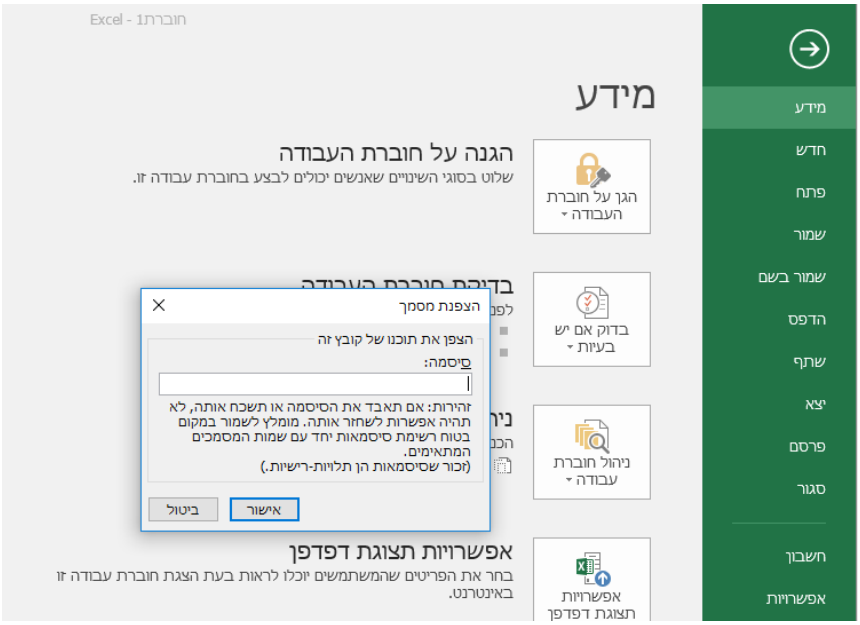
מדינת ישראל
משרד החינוך
מנהל תקשוב טכנולוגיה ומערכות מידע

<u>הגנה על קובץ באמצעות סיסמה</u>

1. בפינה העליונה של הקובץ אקסל יש ללחוץ בפינה הימנית על *"קובץ"*
2. יש ללחוץ על *"הגן על חוברת העבודה"* ולאחר מכן על *"הצפן באמצעות סיסמה"*



3. יש להקיש את הסיסמא שנבחרה ולאחר מכן "אישור", על הסיסמא להיות מורכבת ממינימום 10 תווים הכוללים אות גדולה, אות קטנה ומספר.



4. יש להקיש שוב את הסיסמא שנבחרה
5. יש לשמור את הקובץ בתיקיה במחשב ולשלוח לנמען.
6. את הסיסמא יש לשלוח במייל נפרד.