מדינת ישראל
משרד החינוך
מנהל תקשוב טכנולוגיה ומערכות מידע

סיון תשע״ט
יוני 2019

הנחיות אבטחת מידע למוסדות חינוך

סיכוני אבטחת מידע וסייבר הולכים וגדלים ככל שאמצעים טכנולוגיים הופכים לחלק בלתי נפרד מחיי השגרה שלנו.
על מנת להגן על כל המעורבים במערכת החינוך – תלמידים, עובדי הוראה, משפחות התלמידים, עלינו לוודא שהשימוש בטכנולוגיות מידע בבתי הספר נעשה עם הקפדה על סטנדרט אחיד של אבטחת מידע אשר יאפשר התמודדות עם איומים אלו.
מסמך זה מגדיר את סטנדרט אבטחת המידע לבתי הספר במערכת החינוך ויתעדכן מעת לעת בהתאם לצרכים ולסיכונים

1. הגדרות

א. **מידע מוגן או רגיש**: נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.
לדוגמה: מספר ת״ז, רשימה המכילה פירטי קשר במידה וניתן להבין מהכותרות מידע על התלמידים (כגון רשימת תלמידים בכיתת חינוך מיוחד או תלמידים המקבלים סיוע למעוטי יכולת, תמונה, חוות דעת, אבחון, ציונים, נתונים כספיים)

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.

ד. **הממונה על אבטחת המידע בבית הספר**: אדם הנמנה עם הצוות הקבוע בבית הספר אשר מונה על ידי המנהל לתפקיד זה ואשר אחראי לאבטחת המידע בבית הספר.

2. הנחיות

2.1 האחריות לאבטחת המידע בבית הספר היא של מנהל בית הספר. מנהל בית הספר יכול למנות ממונה אבטחת מידע בית ספרי אשר יפקח על יישום ההנחיות המופיעות במסמך זה.

2.2 **ניהול גישה והרשאות למערכות המכילות מידע על תלמידים**

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

א. משתמשי המערכת לא יעשו שימוש בהרשאות שאינן שלהם וניתנו לבעל תפקיד או לתלמיד אחר.

ב. יש לאסור גישה של תלמידים למערכות ומחשבים מנהלתיים.

2.2.2 במקרה של עזיבת מורה או תלמיד את בית ספר יש לוודא כי הרשאות הגישה שלו למערכות בית הספר ייחסמו באופן מיידי.

2.3 צוות בית הספר יטפל במידע מוגן בהתאם להנחיות משרד החינוך המופיעות בקישור: מדיניות שמירה וטיפול במידע מוגן במוסדות חינוך.

2.4 **שימוש במוצרים חינוכיים טכנולוגיים**
יש לעשות שימוש אך ורק במוצרים חינוכיים טכנולוגיים אותם מספק משרד החינוך ובמוצרים שקיבלו אישור של משרד החינוך;
רשימת המוצרים המאושרים מופיעה ב״קטלוג החינוכי״ בקישור הבא: הקטלוג החינוכי.

2.5 **ניהול והגנת מחשבי בית הספר**

2.5.1 יש לוודא כי על כל המחשבים בבית הספר מותקנת מערכת הפעלה עדכנית שנתמכת על ידי היצרן.

2.5.2 יש לוודא כי לכלל התוכנות המותקנות על מחשבי בית הספר ובכלל זה מערכת ההפעלה רישיון חוקי תקף.

2.5.3 יש לוודא כי מערכת ההפעלה נתמכת על ידי היצרן (כיום Window 7 ומעלה) ומתעדכנת באופן קבוע בעדכוני אבטחת מידע של היצרן. לקבלת רישיון למערכות הפעלה Windows יש ליצור קשר עם מוקד חותם: www.scool.co.il/ness, ובטלפון: 09-8922923.

2.5.4 יש לוודא כי תוכנה להגנה מפני נוזקות (כגון אנטי וירוס) מותקנת על כל המחשבים והשרתים בבית הספר. על תוכנות אלה להתעדכן באופן שוטף ולבצע סריקה יומית לגילוי וניקוי נוזקות.

2.5.5 יש לוודא הגדרת הדפדפנים הפועלים במחשבי בתי הספר, כך שלא ישמרו מידע פרטי, כגון סיסמאות, היסטוריית גלישה ועוד.

2.5.6 יש לוודא כי למשתמשי הקצה אין הרשאות ניהול במחשבים (Local Admin) אשר יאפשרו להם התקנת תוכנות על תחנות הקצה.

2.5.7 במידה ובית הספר מאפשר לסגל החינוכי/תלמידים להוציא מחשבים מחוץ לכותלי בית הספר, יש לוודא נקיטת הפעולות הבאות:
א. אנטי וירוס מבצע סריקה ומתעדכן באופן שוטף.
ב. מערכת ההפעלה מתעדכנת באופן שוטף בעדכוני אבטחת מידע.
ג. לא נשמר או מגובה על המחשב מידע אישי ורגיש.
ד. אבטחת המחשב בכלל ושמירה על המידע בו בפרט.

2.5.8 במקרה שנעשה 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.

2.6 **הגנות רשת**
להלן פירוט הגנות הרשת המינימליות שיש ליישם בבית הספר:

2.6.1 על כלל מערכות המחשב בבית הספר להימצא מאחורי "חומת אש" (FireWall) היקפית אשר מנוהלת ומתוחזקת באופן שוטף, וכי החוקים בה מאפשרים גישה מינימלית למערכות בית הספר, בהתאם לצרכיו.

2.6.2 על מנת לוודא כי לא תהיה גישה ממחשבים שבהם עושים שימוש תלמידים למחשבים ומערכות מנהלתיות, יש להגדיר ב"חומת האש" הפרדה בין הרשת המנהלתית בבית הספר הכוללת את מחשבי המזכירות, מנהל בית הספר וכדומה לבין הרשת הפדגוגית הכוללת את מחשבי המעבדה, כיתות המחשבים וכדומה.

2.6.3 יש לוודא שארונות התקשורת בבית הספר נעולים.

2.6.4 אין לבצע חיבורים לא מורשים לציוד התקשורת הבית ספרי ללא אישור.

2.6.5 בבית ספר שבו קיימת רשת אלחוטית Wi-Fi יש להגדיר את הגישה אליה בסיסמה. את הסיסמא יש לשנות אחת לשנה.

2.7 **שימוש בטוח בדואר אלקטרוני**
לצרכים פדגוגיים ומנהלתיים של בית הספר 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 שבה עושה בית הספר שימוש, כגון Office 365 for Education, G-suit for Education.

2.8 **אתרי אינטרנט**
אתר בית ספרי יוקם בהתאם להנחיות בחוזר מנכ"ל: "שמירת הפרטיות באתרי האינטרנט הבית ספריים".

2.9 **סינון אתרים ותוכן לא ראוי**

יש לוודא כי הגישה מבית הספר לרשת האינטרנט נעשית תמיד באמצעות מנגנוני סינון לחסימת תכנים שאינם ראויים ואתרי אינטרנט זדוניים, כפי שמפורט בחוזר מנכ"ל – חסימת אתרים בלתי רצויים באינטרנט במערכת החינוך:

http://cms.education.gov.il/EducationCMS/applications/mankal/arc/sd9ak3_6_6.htm

2.10 **גיבויים**

2.10.1 יש לוודא כי למידע בבית הספר נעשה גיבוי באופן קבוע למקרה שבו תהיה פגיעה במידע או במערכות המחשוב, וזאת על מנת לחזור לפעילות שוטפת קלה ומהירה.

2.10.2 מערכת הגיבויים תהיה נפרדת ממערכות המחשוב ותמוקם פיזית באזור נפרד ומאובטח שאין אליו גישה של מורים ותלמידים.

2.10.3 יש לבצע אחת לשנה את בדיקת תקינות הגיבויים ויכולת שחזור המידע והמערכות מהם.

2.10.4 אין לבצע את הגיבויים באמצעות מדיה נתיקה, כגון Disk on Key.

2.10.5 גיבויים ב"ענן" – ניתן לבצע גיבויים אך ורק בסביבות "ענן" שאושרו על ידי משרד החינוך.

2.11 **טיפול במידע מודפס**

2.11.1 יש לוודא כי כלל המסמכים בבית ספר המכילים מידע מוגן/חסוי יאוחסנו בחדרים ייעודיים מתויקים בארונות נעולים.

2.11.2 יש לוודא כי מסמכים המכילים מידע מוגן/חסוי יושמדו על ידי גריסה ולא יושלכו לפח.

2.11.3 באזורי קבלת קהל לא יונח על גבי שולחנות מידע רגיש על התלמידים.

2.12 **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 במוסד החינוכי, שימוש במחשבי המוסד החינוכי 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.**