משרד החינוך

המינהל למדע וטכנולוגיה **מינהל תקשוב ומערכות מידע**

נספח אבטחת מידע

גרסה 1 – 15.09.2013

1. מטרה (I)

מסמך זה כולל אוסף דרישות אבטחת מידע לספקי מוצרים חינוכיים טכנולוגיים. עמידה בהוראות מסמך זה היא תנאי סף לקבלת אישור ממשרד החינוך, ועל הספק לעמוד בדרישות אבטחת מידע של משרד החינוך כפי שיעודכנו מעת לעת.

2. הגדרות (I)

2.1. **מידע (מידע מוגן):** נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו.

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

2.3. **מנהל המאגר:** מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה.

2.4. **הממונה על אבטחת המידע אצל הספק:** אדם הנמנה על עובדי הספק אשר מונה על ידי הספק לתפקיד זה ואשר אחראי לאבטחת ה**מידע** הנכלל ב**מאגרי המידע** המצויים בידי הספק וליישום ההנחיות המופיעות במסמך זה.

2.5. **הממונה על אבטחת המידע במשרד החינוך:** אדם שמונה לתפקיד זה מטעם משרד החינוך ואשר אחראי לאבטחת ה**מידע** במשרד החינוך, ואחראי למתן הנחיות אבטחת מידע.

2.6. **נכסי המידע:** כל המידע, מאגרי המידע, נתון אחר או ציוד של משרד החינוך אשר משמש לצורך פעילות המאגר.

2.7. **משתמשי מאגר מידע**

א. כל בעל תפקיד אצל הספק הנדרש מתוקף תפקידו להשתמש במידע אשר נצבר במאגרי המידע של המשרד המצויים אצל הספק או שיש לספק גישה אליהם.

ב. בעלי תפקידים במשרד החינוך המקבלים במסגרת תפקידם דוחות ומידע המופקים ממאגרי מידע של משרד החינוך המצויים בידי הספק או שיש להם גישה אליהם.

ג. מערכות משיקות (צד שלישי) העושות שימוש במידע הנכלל במאגרי המידע של משרד החינוך והמצויים בידי הספק.

2.8. **אבטחה פיזית:** האמצעים הפיזיים הנדרשים להגנה על ציוד המחשוב, לגישה למידע של משרד החינוך ולשרידות המערכות הממוחשבות המכילות את מאגרי המידע.

2.9. "**התקן נייד**" - אחד מאלה:

2.9.1. מחשב המיועד לשימוש נייד **ובכלל זה רד**יו טלפון נייד כהגדרתו בחוק התקשורת (בזק ושידורים) התשמ"ב-1982.

2.9.2. מצע אחר המשמש לאחסון חומר מחשב.

2.10. **סיווג מידע:** הקניית הגדרת רגישות למידע, בהתבסס על העקרונות שהותוו על ידי משרד החינוך והפורום לנושא אבטחת מידע במשרד החינוך.

2.11. **נזק** למידע: פגיעה בסודיות, בשלמות וזמינות המידע בבעלותו של משרד החינוך.

2.12. **אבטחת מידע**": הגנה על סודיות, שלמות וזמינות המידע בבעלותו של משרד החינוך. הגנה על המידע מפני חשיפה, שימוש או העתקה, והכול ללא רשות כדין.

2.13. "**שלמות מידע**": זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין.

2.14. **סודיות המידע**: חשיפת המידע לגורמים לא מורשים.

2.15. **זמינות המידע**: שמירה על נגישות למידע באופן רציף.

2.16. **אירוע במ"מ:** אירוע ביטחון מערכות מחשב; פעולה המתבצעת בזדון או בשוגג. פעולה זו עלולה לפגוע בזמינות, אמינות וסודיות המידע ו/או בציוד המחשוב המשרדי ברמות חומרה שונות, ולהביא להשבתת מערכות, שיבוש נתונים מכוון או חשיפת נתונים לגורמים לא מורשים.

2.17. "**מיקור חוץ**": השימוש בשירותי מיקור חוץ משמעו הוצאה מחוץ לארגון או ביצוע על ידי מי שאינם עובדים בארגון, של פעולות ותהליכים המבוצעים בדרך כלל על ידי הארגון.

2.18. "**מומחה אבטחת מידע**": חברה המתמחה בנושא אבטחת מידע מתוך רשימת הספקים המאושרת על ידי המשרד.

2.19. "**מידע חסוי**": מידע שפגיעה בזמינותו, בשלמותו, באמינותו, בסודיותו או בשרידותו עלולה לגרום לתקלות כגון אלה:

- פגיעה או הכבדה על ביצוע תכניות או פעולות כלכליות, מנהליות, חברתיות, משפטיות ואחרות של המדינה.
- גרימת תקלה לעבודת הגופים הציבוריים שמשמעה עיכוב או ייקור תהליכי עבודה או הפרעה בביצוע אכיפת החוק.
- מידע פנים ארגוני שהנהלת הארגון רוצה לשמור על חשאיותה מול ארגון מתחרה.

3. הנחיות לביצוע (M)

3.1 **סיווג המידע**

אופי הפעילות במשרד החינוך מחייב דגש מיוחד בנושא אבטחת המידע.
משרד החינוך רואה חשיבות רבה במימוש שיטתי ויעיל של היבטי אבטחת המידע במערכות השונות, ובכלל זה היבטים הקשורים להגנה על מידע ולחוק הגנת הפרטיות התשמ"א-1981.

3.2 **סימון המידע**

הספק מתחייב לסמן כל פלט של מידע המופק ממאגרי המידע של המשרד באמצעות כותרת עליונה בנוסח הבא : "מכיל מידע מוגן לפי חוק הגנת הפרטיות - המוסר שלא כדין עובר עבירה"

3.3 **התחייבות הספק**

הספק מתחייב למלא אחר הוראות נספח זה ואחר יתר הוראות המשרד בכל הנוגע לאבטחת מידע, לרבות הוראות אשר יתעדכנו מעת לעת.

3.4 **איומים (I)**

איום פנימי - פגיעה במכוון או בשוגג בשלמות או זמינות או סודיות של נכס מידע של משרד החינוך על ידי גורם בעל הרשאות גישה לאותם נכסים.

איום חיצוני - פגיעה בשלמות או זמינות או סודיות של נכס מידע של משרד החינוך על ידי גורם ללא הרשאות גישה מאושרות לאותם נכסים.

3.5 **גורמי איום עיקריים (I)**

- אדם בעל הרשאות במערכת וללא הרשאות במערכת.
- בעל עניין במידע (אדם/ ארגון/ מדינה), לדוגמה אוכלוסיית מורים ותלמידים.
- גופים עם אינטרסים ועם יכולות – אנשי תקשורת, חוקרים פרטיים, עבריינים קטנים, פשע מאורגן ישראלי ופשע מאורגן בין-לאומי.
- אדם אקראי או גורם נוסף בעל יכולת זדונית.

3.6 **משמעות של מימוש האיומים (I)**

פגיעה בנתוני המערכת עלולה לגרום לנזקים הבאים :

- פגיעה בפעילות התקינה במשרד החינוך כולל זמינות שירותים, אמינות, שלמות וחסינות נתונים.
- פגיעה בצנעת הפרט של עובד המשרד או של אדם מן הציבור ו/או של כל אדם שפרטיו נחשפו מהמערכת.

- הגשת תביעות משפטיות נגד משרד החינוך.
- נזק כלכלי למשרד החינוך.
- נזק תדמיתי בלתי הפיך למשרד החינוך.
- נזק למידע.

3.7. **שימוש, אחזקה או ניהול של מאגרי מידע**

3.7.1. מלוא המידע המצוי במאגרי המידע של המשרד אשר בידי הספק או שיש לספק גישה אליהם, הוא בבעלות המשרד על כל המשתמע מכך. הספק מתחייב שכל גישה שלו, או של מי מטעמו, למידע ולמאגר המידע, תתבצע אך ורק בהתאם להוראות המשרד ולמטרות אשר הוגדרו לו על ידי המשרד.

3.7.2. הספק מתחייב שהוא, או מי מטעמו, יקפיד כי כל איסוף מידע או שימוש בו יבוצע אך ורק בהתאם להוראות החוק והדין, ועל פי הנחיות המשרד.

3.7.3. הספק מתחייב שהוא, או מי מטעמו, לא יעביר מידע, או חלק ממידע, מתוך מאגרי המשרד אשר בידיו או שיש לו גישה אליהם, לצד שלישי כלשהו ללא אישור מפורש ובכתב מאת המשרד.

3.7.4. הספק מתחייב שלא לשמור ולא להוציא מידע של משרד החינוך אל שרתים או משאבי מחשוב אחרים הממוקמים מחוץ לגבולות מדינת ישראל.

3.7.5. הספק מתחייב למנוע שמירה של נתונים רגישים באופן מקומי אצל משתמשי המערכת. במקרים חריגים יש לקבל אישור מפורש ובכתב מהמשרד.

3.7.6. ככל שהספק שומר מידע נוסף כלשהו מעבר למידע אשר הוגדר במפורש על ידי המשרד, עליו לבצע את השמירה ואת ההגנה על המידע בהתאם להוראות החוק, התקנות והנחיות רמו"ט (הרשות למשפט טכנולוגיה ומידע) הרלוונטיות, לרבות בנוגע לרישום מאגרים בהתאם לצורך.

3.8. **זיהוי וניהול סיכונים**

3.8.1. **ניהול הסיכונים**

3.8.1.1. הספק מתחייב לבצע ניהול וזיהוי של סיכוני אבטחת מידע לפי הצורך.

3.8.1.2. הספק מתחייב לפנות למשרד בבקשה לאישור לפני ביצוע שינויים בארכיטקטורת המערכת או באופן מתן השירותים. הספק מתחייב שלא לבצע שינוי כלשהו ללא אישור מפורש ובכתב מהמשרד.

3.9. **הצהרה על מחויבות גורם חיצוני בנושא אבטחת מידע**

הספק יגיש מסמך הצהרה למשרד החינוך, ובו הוא מצהיר על התחייבותו על ביצוע ההנחיות לשמירת אבטחת המידע כפי שמפורט בהנחיות ובמסמכי משרד החינוך.

3.10. ניהול אבטחת מידע ארגונית

3.10.1. הספק מתחייב למנות ממונה אבטחת מידע מטעמו, ואשר יהיה אחראי לאבטחת המידע הנכלל במאגרי המידע המצויים בידי הספק וכן ליישום ההנחיות המופיעות במסמך זה.

3.10.2. הספק יחתום על התחייבות לשמירת סודיות בנוסח שייקבע המשרד, וכן יחתים על התחייבות זו את עובדיו ו/או כל מי מטעמו אשר יהיה בעל גישה למאגר מידע של המשרד או למידע מתוכו.

3.10.3. הספק מתחייב להפריד הפרדה מלאה את מאגרי המשרד המצויים בידיו מיתר מאגרי המידע שברשותו שאינם רלוונטיים לפעילות היישום החינוכי. זאת באמצעות הפרדה לוגית הכוללת סגמנט מבודד מאחורי חומת אש.

3.10.4. בכל מקרה שבו לספק התקשרות עם צד שלישי כלשהו אשר יש לה נגיעה ליישום ההנחיות המפורטות במסמך זה, הספק מתחייב להודיע על כך למשרד ולפעול על פי הנחיותיו וכן ליידע את הצד השלישי על החובות הנובעות מקיום ההנחיות המפורטות במסמך זה.

3.11. אבטחת המידע במישור משאבי האנוש והעובדים

3.11.1. הספק מתחייב כי כל עובדיו ו/או מי מטעמו אשר יהיו בעלי גישה למאגרי המשרד, יהיו בעלי הכשרה מתאימה. בדיקת אימות הרקע של כל מועמד להעסקה כעובד הספק, מי מטעמו או משתמש צד שלישי, תיעשה על ידי הספק כנדרש על פי דין ולפי כללי האתיקה הרלוונטיים, והיקפם יתאים לדרישות המשרד, לסיווג המידע שיהיה נגיש להם ולסיכונים הצפויים.

3.11.2. הספק יהיה אחראי כלפי המשרד לכל פעילות עובדיו ו/או מי מטעמו.

3.11.3. הספק מתחייב שכל עובדיו, ו/או מי מטעמו ו/או משתמשי צד שלישי, מבינים את מלוא האחריות המוטלת עליהם בנוגע למידע ולאבטחתו, וכי הם מתאימים לתפקידים שנועדו להם. על הספק להפחית סיכוני גניבה, הונאה או שימוש לרעה בגישה למידע של המשרד באמצעות נקיטת אמצעי הגנה סבירים ומקובלים (כגון מצלמות אבטחה, תיעוד גישה), וזאת מבלי לגרוע מהוראות נספח זה באשר לאבטחה הפיזית והסביבתית.

3.11.4. הספק מתחייב למנוע מקרים שבהם עובדיו ו/או מי מטעמו ינסו לבצע גישות למאגרים שאליהם לא קיבלו הרשאה. במקרה שבו עובד ו/או מי מטעם הספק ניסה בפעם השלישית לבצע גישה למאגר שאינו מורשה גישה אליו, על הספק למנוע ממנו כל גישה למאגרי המשרד ולדווח על כך מידית למשרד.

3.11.5. הספק מתחייב כי תפקידים ותחומי אחריות של עובדי הספק ו/או מי מטעמו ו/או משתמשי צד שלישי הנוגעים לאבטחה, יוגדרו ויתועדו על ידי הספק לפי מדיניות אבטחת המידע של הארגון.

3.12. אבטחה פיזית וסביבתית

3.12.1. הספק מתחייב כי הגישה לאזורים שקיימים בהם מידע ו/או מאגרי מידע וארונות התקשורת, תהיה מתועדת ומבוקרת באופן המאפשר את וידוא זהות האדם הניגש לציוד שלעיל הכולל מניעת הכחשה. רשומות הכניסה יישמרו למשך שנתיים ויועברו למשרד החינוך לפי דרישה.

3.12.2. בכל מקרה שבו מאגר המידע נמצא ברשות הספק, הספק מתחייב לתעד הכנסה והוצאה של ציוד אל המתקנים שבהם ממוקם המאגר ומהם.

3.12.3. הספק מתחייב כי כניסת ספקים או לקוחות לאזורי חוות השרתים תהיה מבוקרת, תכלול ליווי ותירשם ביומן רישום אירועים.

3.12.4. אמצעים לבקרת כניסה פיזית: הספק מתחייב כי השרתים והציוד המשמש לאחסון, עיבוד וגישה למאגרי המידע והיישומים, יוגנו על ידי אמצעים מתאימים לבקרת כניסה כדי להבטיח שרק לעובדים מורשים תותר הגישה.

3.12.5. הגנה מפני איומים סביבתיים: הספק מתחייב ליישם הגנה פיזית מפני נזקים של שריפה, הצפה, רעידות אדמה, פיצוצים, הפרות סדר וסוגים אחרים של אסונות טבע ופגיעות מעשה ידי אדם.

3.12.6. עבודה באזורים מאובטחים: הספק מתחייב לכתוב וליישם הנחיות לעבודה באזורים מאובטחים.

3.12.7. שירותים תומכים: הספק מתחייב להגן על הציוד בפני הפסקות חשמל והפרעות אחרות הנגרמות בגלל כשל שירותים תומכים.

3.12.8. אבטחת כבלים: הספק מתחייב כי כבלי חשמל ותקשורת הנושאים נתונים או תומכים בשירותי מידע, יוגנו מפני יירוט או נזק.

3.12.9. תחזוקת ציוד: הספק מתחייב לתחזק את הציוד כראוי על מנת להבטיח את זמינותו וכלילותו הרציפות.

3.13. מצעי מידע פיזיים

3.13.1. על הזכיין ליידע את עובדיו וכל מי שנחשף למידע במסגרת התהליכים שבמשרד על חובת יישום ההנחיות לשמירה על מידע מודפס / מצעי מידע פיזיים.

3.13.2. באזורי קבלת קהל לא יאוחסן מידע חסוי. מידע חסוי רגיש לא יונח על גבי שולחנות לקבלת קהל.

3.13.3. מצעי מידע פיזיים (כגון: אמצעי אחסון אלקטרוני או ניירת) האוגרים מידע חסוי - אין להשאירם ללא השגחה, ולאחר שעות העבודה יש לאחסנם במקום נעול.

3.13.4. חל איסור להשאיר פלט המכיל מידע חסוי במדפסות או במכונות צילום. באחריות המדפיס או מצלם המידע לקחת את הפלט מידית.

3.13.5. מידע חסוי אשר השימוש בו הסתיים, חייב לעבור גריסה או להיות מאוחסן בארכיב מאובטח.

3.14. ניהול תקשורת ותפעול

3.14.1. הספק מתחייב להגדיר ולעבוד על פי מערך נוהלי עבודה אשר יתנו מענה לכל דרישות משרד החינוך לרבות בנושא אבטחת מידע.

3.14.2. הספק מתחייב שהנהלים ייבדקו על ידו לפחות פעם בשנה ויתוקנו בהתאם להנחיות משרד החינוך.

3.14.3. אם התגלו ליקויים בעבודת הספק או כתוצאה מגילוי חשיפת אבטחת מידע חדשה, הספק מתחייב לעדכן את נוהלי העבודה ולדווח למשרד החינוך באופן מידי.

3.15. אבטחה לוגית

3.15.1. הספק מתחייב ליישם אמצעי אבטחה הולמים שימנעו חדירה מכוונת או מקרית למערכת או למערכות התשתית והתקשורת.

3.15.2. הספק מתחייב לבצע הפרדה בין רשתות המאכלסות את מאגרי המידע של משרד החינוך ליישומים ולכלל הרשתות (סגמנטציה).

3.15.3. הספק מתחייב שכל אמצעי אבטחת המידע יעברו הקשחות לפי המלצות היצרן.

3.15.4. הספק מתחייב לעדכן באופן שוטף את המערכות השונות למניעת ניצול פרצות אבטחת מידע.

3.15.5. הספק מתחייב שמערכות אבטחת מידע יספקו שרידות מלאה לשמירה על זמינות המערכת.

3.15.6. יש להקפיד על מניעת גישה ללא הזדהות ו/או להצפין ב-SSL ולתייג עמודים בעלי מידע רגיש, וזאת כדי למנוע ממנועי חיפוש חיצוניים לארכב מידע זה ולהנגישו ברשת, ובפרט כל רכיב/עמוד המוגן על ידי סיסמה.

3.16. תיעוד ובקרה

3.16.1. הספק מתחייב לנהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת על מערכות שניגשות למאגרי מידע של המשרד.

3.16.2. הספק מתחייב שבכל פנייה למערכת ולרשומות במאגר יירשמו כל הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

3.16.3. הספק מתחייב שתיעוד הגישה יישמר/יגובה בשרתים נפרדים ממאגר המידע.

3.16.4. הספק מתחייב כי מנגנון הבקרה לא יאפשר ביטול או שינוי של הפעלתו. מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראי אבטחת מידע מטעם הספק ולצוות אבטחת מידע במשרד החינוך.

3.16.5. הספק מתחייב להעביר למשרד החינוך דיווחים תקופתיים ולפי דרישה בכל הנוגע לאופן ניהול מידע אשר נמצא בבעלות המשרד.

3.16.6. הספק מתחייב לדווח באופן מידי לצוות אבטחת מידע במשרד החינוך בכל מקרה של חשש לדליפת מידע מהמאגר או שימוש חורג מההרשאה שניתנה.

3.16.7. הספק מתחייב לשמור את נתוני הרישום של מנגנון הבקרה למשך 24 חודשים לפחות.

3.17. ביקורות אבטחת מידע

3.17.1. הספק מתחייב ליידע את העובדים במאגר בדבר קיומו של מנגנון הבקרה למערכות המאגר והיקף התיעוד המבוצע על ידו.

3.17.2. הספק מתחייב לאפשר למשרד החינוך לערוך ביקורות באתר המארח את המידע.

3.17.3. הספק מתחייב לתקן את הליקויים לפי דוח הביקורת של משרד החינוך בתוך פרק הזמן שייקבע על ידי משרד החינוך.

3.18. ניהול המידע

3.18.1. הספק מתחייב לנהל רשימה של כל נכסי המידע של משרד החינוך שנמצאים ברשותו.

3.18.2. הספק מתחייב להעביר את רשימת כל נכסי המידע של משרד החינוך שנמצאים ברשותו למינהל תקשוב ומערכות מידע.

3.18.3. הספק מתחייב להגדיר ולנהל רשימות מורשים לגישה פיזית לנכסי המידע בבעלות משרד החינוך.

3.18.4. הספק מתחייב שלא להעביר מידע בבעלות משרד החינוך לגורם שלישי ללא אישור בעל המידע במשרד החינוך.

3.18.5. הספק מתחייב לדווח למשרד החינוך על כל צורך בסילוק ציוד מחשוב שכולל מידע בבעלות המשרד. סילוק הציוד יהיה אך ורק באישור גורם מוסמך במשרד החינוך.

3.18.6. אם יש צורך בהשמדת/סילוק מדיה מגנטית, כגון: דיסקים, קלטות גיבוי, מדיה נתיקה מכל סוג, פלט נייר, שכוללת מידע בבעלות משרד החינוך - הספק מתחייב לבער את המידע שבמדיה בהתאם להנחיות ממונה אבטחת מידע במשרד החינוך לאחר גיבוי המידע בהתאם לצורך ולהנחיות המשרד.

3.18.7. הספק מתחייב כי בסיום הפעלת היישום במוסד חינוכי הוא יתאם עם משרד החינוך את השמדת כל נכסי המידע בבעלות משרד החינוך שנשארו ברשותו.

3.19. **ניהול הרשאות גישה**

3.19.1. הספק מתחייב שגישה למערכות המידע ו/או מאגרי המידע תהיה מבוססת על בסיס הצורך לדעת (Need to know), ולא תורשה גישה מעבר לנדרש לצורך מילוי התפקיד כפי שהוגדר על ידי משרד החינוך.

3.19.2. הספק מתחייב לדאוג לגישה ממודרת על בסיס הגדרת תפקידים.

3.19.3. הספק מתחייב לנהל רישום מעודכן של בעלי התפקידים ושל הגישה המוגדרת לכל תפקיד.

3.19.4. הספק מתחייב לגרוע הרשאות לבעלי תפקידים שהסתיים תפקידם או שאין להם צורך במידע שאליו קיבלו הרשאה.

3.19.5. הספק מתחייב לדאוג לבקרות המתאימות על מנת שלא תבוצע גישה לא מורשית למאגרי המידע.

3.19.6. הספק מתחייב שההזדהות למאגרי מידע בעלי רגישות גבוהה תבוצע באמצעות רכיב פיזי בנוסף לסיסמה.

3.19.7. על הספק לזהות את המשתמשים במערכות המידע. במערך ההזדהות תוגדר מדיניות סיסמאות שתכלול לכל הפחות את הפרמטרים הבאים:

- חוזק הסיסמה - לפחות 8 תווים בשילוב של ספרות ואותיות.
- מספר ניסיונות שגויים לנעילה - 3 ניסיונות או לשלב CAPCHA לאחר 3 ניסיונות כושלים.
- שמירת היסטוריית סיסמאות - עד 3 סיסמאות אחורה, איפוס לאחר חצי שנה.
- תדירות החלפת הסיסמה - אחת ל-6 חודשים.

3.19.8. הספק מתחייב לנתק משתמש שהזדהה למערכת מידע לאחר פרק זמן של 20 דקות ללא פעילות.

3.20. **תיעוד אירועי אבטחה**

3.20.1. על הספק לבצע תיעוד של כל אירוע אשר יש בו משום פגיעה בשלמות סודיות וזמינות המידע.

3.20.2. כל אירוע אבטחה ייחקר וייבדק, ויופק דוח אירוע המתאר את הגורמים לאירוע ואת דרכי הטיפול באירוע. הספק יוציא הנחיות לביצוע על מנת להפחית את הסיכוי לאירוע דומה.

3.20.3. על הספק להכין הוראות להתמודדות עם אירועי אבטחת מידע אשר מתייחסים לחומרת האירוע ולמידת רגישות המידע. בהוראות אלו תהיה התייחסות לצעדים מידיים הנדרשים לטיפול באירוע, כגון דיווח למשרד החינוך, ביטול הרשאות.

3.21. **אבטחת תקשורת**

3.21.1. הספק מתחייב לנקוט את אמצעי ההגנה המתאימים על מנת למנוע נזק, פריצה, זיהום או השחתה של מאגרי המידע.

3.21.2. הספק מתחייב שהעברת המידע בתוך רשת התקשורת, ברשת ציבורית או במרשתת תיעשה תוך כדי שימוש בשיטות הצפנה מקובלות.

3.22. **אבטחת תחנות הקצה**

3.22.1. **שמירת מידע רגיש בתחנת הקצה**

חל איסור מוחלט לשמור מידע רגיש בתחנה מרוחקת של המשתמש.

3.23. **הגנה על היישום**

3.23.1. כל שליפת מידע ועדכון נתונים ייבדקו למניעת פגיעה בשרתי מסדי הנתונים, בנתונים ומניעת זיהום הנתונים.

3.23.2. השרתים ימוקמו מאחורי מערך חומות אש ו-IPS למניעת התקפות על היישום מהאינטרנט.

3.23.3. השרתים יוקשחו לפי הגדרות היצרן כולל מערך בקרה.

3.23.4. תצורת השרתים תכלול מערך זמינות על מנת להבטיח גישה רציפה ליישום.

3.24. **התקנים ניידים**

3.24.1. הספק מתחייב שלא להוציא חלקי מידע אל תווך של התקנים ניידים למעט מדיית גיבוי.

3.24.2. אם נדרש מהספק לצורך פעילותו לבצע העלאת חלקי מידע לצורך גיבוי, מתחייב הספק לפנות לקבלת אישור צוות אבטחת המידע במשרד החינוך וכן לנקוט אמצעי הגנה נאותים על מנת להבטיח את שלמות, סודיות וזמינות המידע.

3.24.3. במאגר מידע שניתן להתחבר אליו מרחוק באמצעות המרשתת, הספק מתחייב לבצע זיהוי המונע הכחשה של המורשה לגישה מרחוק. לצורך כך יבוצע שימוש ברכיב פיזי המצוי בשליטתו של המורשה.

3.25. **גיבוי, שחזור והתאוששות**

3.25.1. הספק מתחייב לבצע גיבויים מאובטחים של המידע הנצבר אצלו.

3.25.2. הספק מתחייב לאחסן את מדיית הגיבוי בכספת מוגנת אש ומים הנמצאת מחוץ למתקן המחזיק את מאגרי המידע, או שהספק יעשה שימוש באמצעים שיבטיחו את שלמות המידע ויבטיחו את אפשרות שחזור המידע במקרה של אבדן או הרס.

3.25.3. הספק מתחייב לבצע שחזורים מדגמיים של המדיה המגבה על תשתיותיו לצורך בדיקת ההתאוששות.

3.25.4. הספק מתחייב כי שחזור אמיתי יבוצע באישור מנהל מאגר המידע.

3.25.5. הספק מתחייב כי אם בוצע שחזור אמיתי, יתועדו כל תהליכי השחזור כולל זהותו של מבצע השחזור.

3.25.6. הספק מתחייב למנוע עירוב מידע מסיווגים שונים בזמן השחזור.

3.25.7. לאחר סיום השחזור המדגמי מתחייב הספק למחוק את המידע ששוחזר.