



משרד החינוך

המינהל למדע וטכנולוגיה מינהל תקשוב ומערכות מידע

תקן אבטחת מידע

גרסה 2.5 – 4.12.2016

עדכונים בגרסה 2.5

- נוספו סעיפים 2.23 ועד 2.26 - הגדרות בנושא עננים ציבוריים
- עודכן מסעיף 3.7.4 עד סעיף 3.7.10 כולל שינוי מספרי סעיפים והוספת סעיפים - בנושא מתן אפשרות להוצאת מידע של משרד החינוך ו/או המוסד החינוכי אל שרתים או משאבי מחשוב אחרים הממוקמים מחוץ לגבולות מדינת ישראל.
- עודכן סעיף 3.19.8 - דרישות בנושא הזדהות
- נוסף סעיף 10 - דרישות מספק השירות מחוץ לגבולות מדינת ישראל למידע מוגן וחסוי.
- שונה מס' סעיף 10 - תחולה - לסעיף מס' 11.

עדכונים בגרסה 2.4

- עודכן סעיף 3.7.5 - בנושא מתן אפשרות להוציא מידע מוגן מתוך המערכת.
- עודכן סעיף 6 - הכותרת שונתה ל"דגשים לאפליקציית מובייל", והוחלף המינוח מיישום לאפליקציה.
- עודכן סעיף 6.2 - הכותרת שונתה ל"הזדהות באפליקציית מובייל" ועודכנו תתי-סעיפים בנושא הנחיות לגבי הזדהות באפליקציית מובייל.
- עודכן סעיף 7 - נוספו תתי-סעיפים 7.1.8 ו-7.1.9 בנושא הנחיות לגבי שימוש בתוכנת השתלטות לתמיכת הלקוחות, ושוננו מספרי תתי-סעיפים.
- נוסף סעיף 9 - גביית תשלומים - בנושא הנחיות לגבי גביית תשלומים דרך המערכת.
- שונה מס' סעיף 9 - תחולה - לסעיף מס' 10.

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. על הספק לעמוד בדרישות אבטחת מידע של משרד החינוך כפי שיעודכנו מעת לעת בקישור:

http://sites.education.gov.il/cloud/home/meyda_le_sapakim/Documents/TekeAVTAM.pdf

בשאלות הקשורות לתקן אבטחת מידע אפשר לפנות אל גב' שני נחום,

רכזת צוות בדיקות טכנולוגיות, טל': 03-7407215 או בדוא"ל:

pniot_tech@education.gov.il

2. הגדרות (I)

- 2.1 **מידע (מידע מוגן):** נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו וכדומה, לדוגמה: ת"ז, תמונה.
- 2.2 **מאגר מידע:** אוסף נתוני **מידע** המוחזק באמצעי מגנטי או אופטי (ובכלל זה מחשב) או פלט מודפס, ומיועד לעיבוד ממוחשב.
- 2.3 **תשתיות:** כל החומרה והתוכנה שעליהן פועל מאגר המידע/המערכת.
- 2.4 **מנהל המאגר:** מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה.
- 2.5 **הממונה על אבטחת המידע אצל הספק:** אדם הנמנה על עובדי הספק אשר מונה על ידי הספק לתפקיד זה ואשר אחראי לאבטחת המידע הנכלל במאגרי המידע והתשתיות המצויים בידי הספק וליישום ההנחיות המופיעות במסמך זה.
- 2.6 **הממונה על אבטחת המידע במשרד החינוך:** אדם שמונה לתפקיד זה מטעם משרד החינוך ואשר אחראי לאבטחת המידע במשרד החינוך, ואחראי למתן הנחיות אבטחת מידע.

- 2.7. **נכסי המידע:** כל המידע, מאגרי המידע, נתון אחר או ציוד של משרד החינוך אשר משמש לצורך פעילות המאגר.
- 2.8. **מצב חירום:** מצב זה מוגדר ומוכרז רשמית על ידי הגורמים המוסמכים לכך במדינה. במצב זה יש שמוגבלת הפעילות הלימודית הסדירה במוסדות החינוך לתקופת זמן של כמה ימים עד שבועות אחדים.
- 2.9. **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.
- 2.10. **אבטחה פיזית:** האמצעים הפיזיים הנדרשים להגנה על ציוד המחשוב, לגישה למידע של משרד החינוך ולשרידות המערכות הממוחשבות המכילות את מאגרי המידע.
- 2.11. **"התקן נייד"** - אחד מאלה:
- 2.11.1. מחשב המיועד לשימוש נייד **ובכלל זה רדיו** טלפון נייד כהגדרתו בחוק התקשורת (בזק ושידורים) התשמ"ב-1982.
- 2.11.2. מצע אחר המשמש לאחסון חומר מחשב.
- 2.12. **סיווג מידע/מערכת:** הקניית הגדרת רגישות למידע/מערכת, בהתבסס על העקרונות שהותוו על ידי משרד החינוך והפורום לנושא אבטחת מידע במשרד החינוך. להלן פירוט הסיווגים:
- 2.12.1. **בלמ"ס** – מערכת שאינה שומרת ו/או מעבדת מידע מוגן.
- 2.12.2. **מוגן** – מערכת השומרת ו/או מעבדת מידע מוגן.
תת סיווג:
- 2.12.3. **חסוי** – מערכת השומרת ו/או מעבדת מידע חסוי.
- 2.13. **נזק למידע:** פגיעה בסודיות, בשלמות ובזמינות המידע בבעלותו של משרד החינוך.

- 2.14. "אבטחת מידע": הגנה על סודיות, שלמות וזמינות המידע בבעלותו של משרד החינוך. הגנה על המידע מפני חשיפה, שימוש או העתקה, והכול ללא רשות כדין.
- 2.15. "שלמות מידע": זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששנו, נמסרו או הושמדו ללא רשות כדין.
- 2.16. **סודיות המידע**: חשיפת המידע לגורמים לא מורשים.
- 2.17. **זמינות המידע**: שמירה על נגישות למידע באופן רציף.
- 2.18. **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.
- 2.19. "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.
- 2.20. "מומחה אבטחת מידע": חברה או אדם פרטי, או גוף אחר המתמחה בנושא אבטחת מידע מתוך רשימת הספקים המאושרת על ידי המשרד.
- 2.21. "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.
- 2.22. "הצפנה": הצפנת הנתונים בשיטה שתאפשר על ידי המשרד, ושלא תאפשר פיצוח המידע על ידי גורם חיצוני לאפליקציה.
- 2.23. **ענן מחשוב או מחשוב בענן** (באנגלית: Cloud computing): שירותי מחשוב הניתנים למשתמש באמצעות שרתים מרוחקים שאליהם מתחבר המשתמש, בדרך כלל רשת האינטרנט.
- 2.24. **ענן ציבורי** (באנגלית: **Public Cloud**): שירות המאחד כמה ארגונים (לקוחות) על תשתית מרכזית אחת.

2.25. **IaaS - תשתית כשירות (Infrastructure as a Service)**: היכולת הניתנת בידי הלקוח להקצות, לעבד, לאחסן ולהשתמש במשאבים מחשוביים בסיסיים אחרים שעליהם הלקוח רשאי להריץ תוכנות כרצונו. ללקוח אין שליטה על התשתית עצמה, לרבות שרתים, אחסון והתקני תקשורת, אך יש לו שליטה על כל מה שמוחקן על תשתית זו.

2.26. **הזדהות חזקה** (כזו המאפשרת רמת ודאות גבוהה במיוחד בזיהוי) תכלול שילוב של שתיים מתוך שלוש הקבוצות:

- 2.26.1. משהו שהשתמש יודע - בקבוצה זו נכללות סיסמאות.
- 2.26.2. משהו בבעלות המשתמש - בקבוצה זו נכללים מנגנוני ייצור סיסמה חד-פעמית (OTP), רכיבי אחסון לסיסמאות (Token), כרטיסים חכמים ועוד.
- 2.26.3. משהו שהוא המשתמש - בקבוצה זו נכללים אמצעי הזיהוי הביومترיים.

3. הנחיות לביצוע (M)

3.1. סיווג המידע/המערכת

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.

סעיפי ההנחיות מסומנים באופן הבא:

בלמ"ס – ללא סימון

רגיש – עם סימון (רגיש) בכותרת הסעיף

לכל אחד מהסיווגים לעיל יכולה להצטרף סיומת: חסוי – עם סימון (חסוי) בכותרת הסעיף.

יש לממש את הסעיפים באופן הבא לפי סיווג המידע/המערכת:

בלמ"ס – כל סעיפי בלמ"ס (ללא סימון)

מוגן – כל סעיפי בלמ"ס, ומוגן

תת סיווג: חסוי – כל סעיפי חסוי בנוסף להגדרת הסיווג

3.2. (חסוי) סימון המידע

הספק מתחייב לסמן כל פלט של מידע המופק ממאגרי המידע של המשרד באמצעות כותרת עליונה בנוסח הבא: "מכיל מידע מוגן/חסוי 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 במערכת ובנתונייה עלולה לגרום לנזקים הבאים:
- פגיעה בפעילות התקינה במשרד החינוך כולל זמינות שירותים, אמינות, שלמות וחסינות נתונים.
 - פגיעה בצנעת הפרט של עובד המשרד/הוראה או של אדם מן הציבור ו/או של כל אדם שפרטיו נחשפו מהמערכת.
 - הגשת תביעות משפטיות נגד משרד החינוך ומוסדות חינוך.
 - נזק כלכלי למשרד החינוך ומוסדות חינוך.
 - נזק תדמיתי בלתי הפיך למשרד החינוך ומוסדות חינוך.
 - נזק למידע.

3.7 (מוגן) שימוש, אחזקה או ניהול של מאגרי מידע

- 3.7.1 . מלוא המידע המצוי במאגרי המידע של המשרד ו/או נאסף או נוצר במסגרת פעילות של המשרד או מוסדות חינוך 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 בידי או שיש לו גישה אליהם, לצד שלישי כלשהו ללא אישור מפורש ובכתב מאת המשרד.
- 3.7.4 . מיקום גיאוגרפי של המידע והשרתים או משאבי מחשוב המאחסנים מידע:
- 3.7.4.1 . הוצאת מידע של משרד החינוך ו/או המוסד החינוכי אל שרתים או משאבי מחשוב אחרים הממוקמים מחוץ לגבולות מדינת ישראל תתאפשר בהתאם לעמידה בדרישות המפורטות במסמך ודרישות שבסעיף 10 במסמך זה ותוך כדי נקיטת אמצעים שלא יפחתו מהמפורט בתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001.
- 3.7.4.2 . בשלב זה תאושר העברת מידע רק למדינות החברות באיחוד האירופי.
- 3.7.4.3 . יש להבטיח בכתב כי מקבל המידע נוקט אמצעים מספיקים להבטחת פרטיותם של מי שהמידע עליהם, וכי הוא מבטיח שהמידע לא יועבר לאף גורם זולתו, בין שבאותה מדינה ובין שבמדינה אחרת.
- 3.7.4.4 . למען הסר ספק, ניתן לאחסן שירותים בשירותי ענן שאינם ממוקמים בישראל, אך לא כאלה המאחסנים מידע מוגן/חסוי.
- 3.7.4.5 . על הספק להציג למשרד החינוך דוגמת תיעוד (LOG) מתוך מערכות התשתית ואבטחת מידע של הענן לרבות הפרטים הבאים: תאריך, שעה, זהות הגישה, כתובת IP, מהות הגישה, אם נדחתה או אושרה.

- 3.7.5 . אם נדרש להוציא מידע מוגן מתוך המערכת, יש לפעול לפי ההנחיות הבאות :
- 3.7.5.1 . יש לאפשר הוצאת מידע רלוונטי בלבד, לדוגמה – לאשר הוצאת רשימת תלמידים בבית הספר/כיתה, אך לא לאפשר הוצאת רשימת תעודות זהות, אם לא נדרש.
- 3.7.5.2 . יש להציג הודעה למשתמש לפני הוצאת המידע מהמערכת בנוסח הבא :
- "המידע המופק מתוך המערכת מכיל מידע המוגן על פי חוק הגנת הפרטיות. יש לשמור את המידע במקום מוגן שלא יאפשר גישה לא מורשית למידע.
- אין להעתיק, להפיץ, להציג או למסור לצד שלישי את המידע או חלק ממנו. המוסר את המידע שלא כדין עובר עבירה".
- 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 רמ"ט (הרשות למשפט, טכנולוגיה ומידע) הרלוונטיות, לרבות בנוגע לרישום מאגרים בהתאם לצורך.
- 3.8 . **זיהוי וניהול סיכונים**
- 3.8.1 . הספק מתחייב לבצע ניהול וזיהוי של סיכונים אבטחת מידע לפי הצורך.
- 3.8.2 . הספק מתחייב לפנות למשרד בבקשה לאישור לפני ביצוע שינויים מהותיים 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 לביצוע 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 במערכת ומאגרי המידע המצויים בידי הספק וכן ליישום ההנחיות המופיעות במסמך זה.
- 3.10.2 . הספק יחתום על התחייבות לשמירת סודיות בנוסח שיקבע 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. (חסוי או מוגן) 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. (חסוי או מוגן) 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. (מוגן) הספק מתחייב כי כל עובדיו ו/או מי מטעמו אשר יהיו בעלי גישה למאגרי המידע או המערכת, יהיו בעלי הכשרה מתאימה. בדיקה ואימות הרקע של כל מועמד להעסקה כעובד הספק, מי מטעמו או משתמש צד שלישי, ייעשו על ידי הספק כנדרש על פי כל דין, ובכלל זה החוק למניעת העסקת עברייני מין התשס"א-2001, ולפי כללי האתיקה הרלוונטיים והיקפם יתאים לדרישות המשרד, לסיווג המידע שיהיה נגיש להם ולסיכונים הצפויים, כולל לעניין חשיפת המידע בפני העובד בהתחשב ברקע שלו.

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 למערכת, למידע ולאבטחתם, 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 מיידית 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. (מוגן או חסוי) 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. (מוגן או חסוי) 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 ייתנו 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 מידתי.

3.15. אבטחה לוגית

3.15.1. כל הסעיפים הבאים מתייחסים לסביבת הפיתוח, הבדיקות והייצור.

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

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 ולתייג עמודים בעלי מידע רגיש, וזאת כדי למנוע ממנועי חיפוש חיצוניים לארכב מידע זה ולהנגישו ברשת.

3.15.7. יש להקפיד על הצפנה ב-SSL לעמודים בעלי מידע רגיש, ובפרט כל רכיב/עמוד המוגן על ידי סיסמה.

3.15.8. למען הסר ספק, גם אם הספק מתארח בחוות הדעת של משרד החינוך, חובתו לוודא כי בקרות אבטחת מידע הרלוונטיות מיושמות בצורה המתאימה ליישום שאותו הוא מארח בענן.

3.16. (מוגן או חסוי) תיעוד ובקרה

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

3.16.2. הספק מתחייב שבכל פנייה למערכת ולרשומות במאגר יירשמו כל הנתונים הבאים: זהות המשתמש, כתובת IP, 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.

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. ביקורת 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. (מוגן או חסוי) 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 מחשב שכולל מידע בבעלות המשרד. סילוק הציוד יהיה אך ורק באישור גורם מוסמך במשרד החינוך. למען הסר ספק, סעיף זה רלוונטי גם לספקים המתארחים בחוות הדעת של משרד 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. למען הסר ספק, סעיף זה רלוונטי גם לספקים המתארחים בחוות הדעת של משרד החינוך.

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. למען הסר ספק, סעיף זה רלוונטי גם לספקים המתארחים בחוות הדעת של משרד החינוך.

3.18.8. הספק מתחייב שכל מידע אשר מועבר ממוסד החינוך אליו ובחזרה יועבר בצורה מאובטחת ועל פי דרישות ולאחר אישור משרד החינוך.

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 לא יאוחר מ-72 שעות מסיום התפקיד.
- 3.19.5. הספק מתחייב לדאוג לבקורות המתאימות על מנת שלא תבוצע גישה לא מורשית למאגרי המידע.
- 3.19.6. הספק מתחייב שההזדהות לניהול מאגרי מידע בעלי רגישות גבוהה תבוצע באמצעות רכיב פיזי בנוסף לסיסמה.
- 3.19.7. מערכות לניהול פדגוגי אשר מבצעות התממשקות לשרתי משרד החינוך או למערכות משרד החינוך, מחויבות לבצע קריאות מאובטחות באמצעות SSL תוך כדי שימוש בתעודות עם מפתח ציבורי ופרטי אשר מונפקות על ידי CA מאושר.
- 3.19.8. על הספק לזהות את המשתמשים במערכות המידע. במערך ההזדהות תוגדר מדיניות סיסמאות שתכלול לכל הפחות את הפרמטרים הבאים:
- שם המשתמש יכלול לפחות 5 תווים.
 - אין לזהות את סגל ההוראה ובעלי תפקיד במוסד החינוכי באמצעות מספר תעודת הזהות, לא כשם משתמש ולא כסיסמה.
 - יש לפעול לזיהוי כלל המשתמשים במערכת למעט סגל ההוראה ובעלי תפקיד במוסד החינוכי בהתאם [להנחיה מספר 1-2010](#) של רמ"ט במשרד המשפטים.
 - חוזק הסיסמה – לתלמידים: לפחות 6 תווים; כל משתמש אחר, לרבות מנהל מערכת: לפחות 8 תווים, בשילוב של ספרות ואותיות. לא יותר מ-16 תווים.
 - מספר ניסיונות שגויים לנעילה – 5 ניסיונות או לשלב CAPTCHA לאחר 3 ניסיונות כושלים.

- יש להציג רכיב CAPTCHA גם בטפסים רגישים, כגון החלפת סיסמאות, עדכון פרטים אישיים וכיוצא באלה, לאחר 3 ניסיונות כושלים.
- פרק זמן לנעילה לאחר ניסיונות כושלים – 10 דקות.
- שמירת היסטוריית סיסמאות – עד 3 סיסמאות אחורה לכלל המשתמשים ולתלמידים עד סיסמה אחת אחורה, איפוס לאחר שנה.
- תדירות החלפת הסיסמה – לתלמידים אחת לשנה, לשאר המשתמשים אחת ל-6 חודשים.
- סיסמה ראשונית – אקראית ושונה בין משתמש למשתמש. המשתמש יידרש לשנות את הסיסמה בכניסה הראשונה.
- 3.19.9. הספק מתחייב לנתק משתמש שהזדהה למערכת המידע לאחר פרק זמן של 60 דקות ללא פעילות, ואחרי פרק זמן של 10 שעות בפעילות רצופה.
- 3.19.10. להלן מדיניות הסיסמאות עבור תלמידים במערכות המיועדות לשכבות גיל של גני ילדים עד כיתה א' (כולל) וכן חינוך מיוחד, ובתנאי שהמידע במערכת אינו מידע מוגן:
- חוזק סיסמה – 4 מספרים/תווים לא עוקבים, וביניהם לא יהיו 3 מספרים/תווים זהים ברצף.
- מספר ניסיונות שגויים לנעילה – 7 ניסיונות או לשלב CAPTCHA לאחר 4 ניסיונות כושלים; מומלץ CAPTCHA המורכב ממספרים. שחרור נעילה אוטומטי לאחר 10 דקות.
- תדירות החלפת הסיסמה – עד אחת ל-24 חודשים.
- ניתן להציע גם שיטות זיהוי אלטרנטיביות המבוססות על מחוות/תמונות, בכפוף לאישור המשרד. רמת האבטחה מבחינת פרמוטציות וכדומה לא תהיה פחותה מזאת הנדרשת על ידי רמת האבטחה לפי מדיניות הסיסמאות הרלוונטית שתוארה לעיל.
- 3.19.11. **איפוס סיסמאות**
- הספק יכול לבחור בין אחת או יותר מהחלופות הבאות:
- איפוס סיסמה בשירות עצמי (Self Service) תוך כדי שימוש בכתובת דוא"ל / טלפון נייד.
- איפוס סיסמה באמצעות מינהלן בבית ספר.

3.19.12. **העברת מידע ממוסד חינוך למתן הרשאות** – אין לדרוש ממוסד חינוך להעביר מידע אישי, לרבות: ת"ז, כתובת, טלפונים, תמונה, מגדר, שמות הורים וכיוצא באלה, במטרה לתת הרשאה למערכת.

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.

3.20.4. על הספק להעביר למשרד החינוך את דוח האירוע בתוך 72 שעות מקרות האירוע, ואת ההנחיות בתוך 21 יום מקרות האירוע. למשרד החינוך שמורה הזכות להוסיף, לגרוע או לעדכן את המסמכים שיועברו, וכן לזמן את הספק לתחקור האירוע והפקת לקחים.

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. (מוגן) אבטחת תחנות הקצה

3.22.1. שמירת מידע מוגן בתחנת הקצה

חל איסור מוחלט לשמור מידע מוגן בתחנה מרוחקת של המשתמש.

3.23. הגנה על היישום

3.23.1. כל שליפת מידע ועדכון נתונים ייבדקו למניעת פגיעה בשרתי מסדי הנתונים, בנתונים ולמניעת 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. (מוגן) 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. (חסוי) ניטור

3.25.1. הספק ינטר את התעבורה ברכיבי התקשורת באופן שוטף בסביבות העבודה השונות.

3.25.2. הספק ינטר את רכיבי החומרה והתוכנה באמצעות כלי ניטור בקרה וניהול, יזהה עומסים ונקודות כשל ויטפל בהם, וכן יתאים את המערכת לעמידה בעומסים הצפויים.

3.25.3. משרד החינוך שומר לעצמו את הזכות לבקש דוחות זמינות ועומסים בתשתיות וביישומים לא יותר מאחת לחודש, למעט במצב חירום או תרגיל.

3.26. שרידות וזמינות

3.26.1. (חסוי) על הספק ליישם מערכות שיאפשרו שרידות מלאה של כל רכיבי התשתית.

3.26.2. על המערכות להיות זמינות 24X7, למעט חריגים דוגמת המגזר החרדי.

3.26.3. השבתה

3.26.3.1. השבתת המערכת לצורך תחזוקה ועדכון תיעשה בשעות הלילה או

שעות אחרות שבהן אין פעילות במערכת (חופשות, חגים, סופי

- שבוע וכיוצא באלה), ובכל מקרה ההשבתה תסתיים שעתיים לפני תחילת הפעילות במערכת.
- 3.26.3.2. אין לבצע יותר משתי השבתות בחודש, אלא אם כן התקבל אישור ממשרד החינוך מראש.
- 3.26.3.3. אין לבצע השבתות במצב חירום או בזמן תרגיל.
- 3.26.3.4. ההשבתה תיעשה תוך כדי הודעה למנהל האתר והודעה באתר עצמו במקום בולט טרום ההשבתה, וכן במהלכה.
- 3.26.4. זמן התאוששות לכל רכיבי התשתית, השרתים והמידע – בתוך 8 שעות לכל היותר למערכות המסווגות חסוי, ו-72 שעות לשאר המערכות.
- 3.26.5. על מנת להיות מסוגל לעמוד בהרחבת התשתית של השרתים שעליהם מותקנת הסביבה, על היצרן להצהיר לגבי יכולת הרחבה פיזית או וירטואלית של שרתים.
- 3.26.6. (חסוי) שרתי האינטרנט – על הספק ליישם מנגנון איזון עומסים ושרידות של שרתי האינטרנט ולעמוד בעומסים הנדרשים לפי דפוסי השימוש.
- 3.26.7. (חסוי) שרידות מסדי הנתונים – CLUSTER של הנתונים עם חיבור לשרתים במצב של ACTIVE/PASSIVE או ACTIVE/ACTIVE.
- 3.26.8. (חסוי) שרידות מערכות אבטחת המידע – על הספק ליישם מנגנון שרידות למערכות FIREWALL.
- 3.26.9. (חסוי) שרידות קווי התקשורת – על הספק ליישם מנגנון איזון עומסים אוטומטי וזמינות לקווי התקשורת. כמו כן עליו להציג יכולת לנתב/להשבית אפליקציות בתוך הסביבה בעת עומס.
- 3.26.10. על היצרן להתחייב לעמוד בלפחות 30% מהעומס בתקופות של פעילות רגילה של המערכת.
- 3.26.11. **בדיקות עומסים**
- 3.26.11.1. על היצרן לבצע עצמאית בדיקות עומסים יזומות של הסביבה לפחות פעם בשנה ולהציג למשרד את תוצאות הבדיקה כתנאי לקבלת האישור. הניטור צריך לכלול את הנתונים הבאים: רוחב פס, עומס מעבד, עומס זיכרון, שאילות מול בסיסי הנתונים, פניות בו זמנית לשרת WEB. על היצרן להציג את כלי הניטור שבהם השתמש לבדיקת העומסים.

3.26.11.2. על היצרן להציג את הנתונים הבאים של הסביבה כאשר העומס הוא של 100% מהמשתמשים הרשומים במערכת:

- זמני תגובה.
- נפילות שרתים ושירותים של הסביבה.
- דרכי התמודדות עם כשלים ונפילות שרתים ושירותים.

3.26.12. נוהלי חובה בעת כשל/נפילת מערכת

3.26.12.1. על היצרן להעביר חיווי בדוא"ל ובהודעות טקסט לגורמים (לפחות שניים) האחראים מטעמו לזמינות ושירות הסביבה, וזאת כאשר הסביבה נופלת, או כאשר יש עומס חריג על השרתים הפוגע בזמני התגובה הרגילים של המערכת.

3.26.12.2. על היצרן להודיע על האירוע למשרד החינוך עד 60 דקות מגילוי התקלה באמצעות דוא"ל, ולספק פרטי איש קשר שמולו יוכל המשרד להתעדכן.

3.26.12.3. על היצרן להודיע למשתמשים על התקלה באמצעות הודעה במסך הראשי של המוצר לא יאוחר מ-60 דקות מגילוי התקלה. מומלץ להודיע גם למנהלי המערכת בבית הספר באמצעות דוא"ל/הודעת טקסט.

3.26.12.4. על היצרן לספק למשרד לפי דרישה את כל המידע הרלוונטי המצוי לגבי נסיבות הנפילה, וכיצד פעל על מנת להשיב את המערכת למצב תקין, לרבות העומסים בעת התקלה, כמויות משתמשים רשומים וכיוצא באלה.

3.27. (מוגן או חסוי) גיבוי, שחזור והתאוששות

3.27.1. הספק מתחייב לבצע גיבויים מאובטחים של המערכות והמידע הנצבר אצלו באופן כזה שיבטיח התאוששות של המערכת והמידע בתוך 8 שעות מקרות המקרה.

3.27.2. המידע המשוחזר צריך להיות עדכני עד 24 שעות לפני קרות המקרה.

3.27.3. 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 אובדן או הרס.

- 3.27.4. הספק מתחייב לבצע שחזורים מדגמיים של המדיה המגבה על תשתיותיו לצורך בדיקת ההתאוששות.
- 3.27.5. הספק מתחייב כי שחזור אמיתי יבוצע באישור מנהל מאגר המידע.
- 3.27.6. הספק מתחייב כי אם בוצע שחזור אמיתי, יתועדו כל תהליכי השחזור כולל זהותו של מבצע השחזור.
- 3.27.7. הספק מתחייב למנוע עירוב מידע מסיווגים שונים בזמן השחזור.
- 3.27.8. לאחר סיום השחזור המדגמי מתחייב הספק למחוק את המידע ששוחזר.

3.28. אבטחת מידע אפליקטיבית

- 3.28.1. הספק מתחייב כי הקוד מפותח לפי כללי האצבע הבאים :

נושא	כלל האצבע
בדיקת קלט ונתונים	<ul style="list-style-type: none"> • בדוק תקינות של Input ,QueryStings ,Cookies ,Http Headers. • אל תסמוך על בדיקות צד לקוח, יש תמיד לבדוק גם בצד שרת. • יש לבדוק גודל, תקינות וחוקיות של קלט. • עשה שימוש ב-Regular expression validators. • בדוק במיוחד קלט אשר משמש כפרמטר לשאילתות SQL כדי למנוע Sql Injection.
הזדהות	<ul style="list-style-type: none"> • בצע חלוקה של המערכת לאזורים פתוחים ואזורים הדורשים הזדהות. • עשה שימוש בסיסמאות חזקות. • אל תשמור סיסמאות בצורה גלויה. • עשה שימוש במנגנון פג תוקף של סיסמאות ו-Password Policy.
הרשאות	<ul style="list-style-type: none"> • בצע בדיקות הרשאות לפי שייכות המשתמש לתפקידים. • הגבל גישה למשאבי מערכת למשתמשים מורשים בלבד.
מידע רגיש	<ul style="list-style-type: none"> • אל תשמור סיסמאות כ-Clear Text. • שמור מידע רגיש במקומות בטוחים בלבד. • עשה שימוש בתשתית Encryption / Decryption סטנדרטית ואל תפתח מנגנונים עצמיים (SSL). • אין להשאיר בסביבת הייצור קובצי פיתוח, בדיקות וקבצים שלא למטרת היישום בסביבת הייצור (כגון *.back * וכדומה). • יש להגביל ברמת היישום שמירת סיסמאות וזהויות על ידי

נושא	כלל האצבע
	הדפדפן.
ניהול Session	<ul style="list-style-type: none"> קצר את משך זמן ה-Idle ככל שניתן ולא יותר משעה. בכל מקרה, זמן הפעילות ב-Session לא יעלה על 8 שעות.
ניהול Exceptions	<ul style="list-style-type: none"> עשה שימוש ב-Try Catch בצורה מושכלת במערכת. אל תגלה מידע טכני משגיאות אשר נותן מידע לתוקף, עשה שימוש בדפי שגיאה כלליים. שמור ב-Log שגיאות. בכל שגיאה סגור את ה-Session.
Audit & Log	<ul style="list-style-type: none"> עשה שימוש במנגנון Log ו-Audit מרכזי.
Asp.Net	<ul style="list-style-type: none"> עשה שימוש במנגנון Url Authorization לדפים ומחיצות.
Dal / פנייה לבסיס הנתונים	<ul style="list-style-type: none"> עשה שימוש ב-Command parameters כדי למנוע Sql Injection.
מניעת התקפת BOTNET	<ul style="list-style-type: none"> הגדרת NOROBOT ב-Web Server לעמודים המכילים מידע רגיש.

- 3.28.2 (חסוי, מוגן) הספק מתחייב לבצע בדיקות חוסן באמצעות חברה חיצונית בלתי תלויה המומחית בבדיקות חוסן אפליקטיביות, ובעלת ניסיון של לפחות 5 שנים, ולפחות שני לקוחות בסדר גודל של מעל 1000 משתמשים. בדיקות אלה יבוצעו לא על נתוני אמת של המערכת המקורית. אם קיים צורך בהעתקת נתונים ממערכות הייצור – יש לשנות את נתוני הזיהוי על מנת להבטיח שלא תהיה גישה למידע על הפרט או מידע רגיש אחר של משרד החינוך. את הבדיקה יש לבצע אחת לשנה או בכל שינוי מהותי ביישום הקיים.
- 3.28.3 הספק מתחייב לשמור בצורה מאובטחת את גרסאות הקוד שפיתח.
- 3.28.4 הספק מתחייב שלא ישמור גרסאות קודמות של הקוד במערכות הייצור.
- 3.28.5 אין להשתמש בקוד שיווק מחדש Remarketing Code (לדוגמה של הרשת החברתית פייסבוק, גוגל ואחרים) באתרים ודפי אינטרנט.

4. אירוח אצל ספקי אירוח (ISP) או חוות הדעת

למען הסר ספק, אם הספק מתארח אצל ספק אירוח חיצוני, כולל חוות הדעת, חובתו לוודא שכל בקורות אבטחת המידע והדרישות בתקן זה מיושמות בהתאם ליישום הרלוונטי.

5. סביבת הפיתוח אצל הספק

המידע שנועד לשימוש בסביבת הפיתוח, יהיה מידע לא מזוהה ושאינו מכיל מידע מוגן.

6. דגשים לאפליקציות מובייל

6.1 שמירת מידע על המכשיר

- 6.1.1 האפליקציה לא תשמור מידע מוגן או חסוי במכשיר ללא הצפנת הנתונים.
- 6.1.2 האפליקציה תאפשר למשתמשים למחוק את כל הנתונים הקשורים אליה באופן פשוט וברור.
- 6.1.3 האפליקציה יכולה להשתמש בזיכרון המכשיר לשמירת מידע כל עוד הוא איננו מאפשר לאפליקציות אחרות גישה למידע, ובתנאי שהמידע מוצפן, לרבות נתוני הזדהות.

6.2 הזדהות באפליקציות מובייל

- 6.2.1 הגישה לאפליקציה המכילה מידע מוגן מחייבת הזדהות לפי דרישות תקן אבטחת מידע.
- 6.2.2 אין לאפשר כניסה אוטומטית לאפליקציה באמצעות שמירת זהות המשתמש והסיסמה ("זכור אותי") לאזורים המכילים מידע מוגן/חסוי, למעט המידע האישי של מחזיק המכשיר הסלולרי. למען הסר ספק, באזורים באפליקציה המאפשרים גישה ו/או ניהול של זהויות רבות יש צורך בהזדהות.
- 6.2.3 כעיקרון, ההזדהות חייבת להתבצע מול שרת מרוחק ולא באופן מקומי על המכשיר. ניתן לאפשר הזדהות מקומית לזמן מוגבל של עד 5 שעות ליום עם זמן Idle של 10 דקות.
- 6.2.4 התקשורת בין האפליקציה לשרת ההזדהות צריכה להיות מוצפנת ומאובטחת.
- 6.3 שימוש בנתונים**
- 6.3.1 שימוש באמצעות האפליקציה לגישה לנתונים השמורים במכשיר, כגון אנשי קשר, תמונות ופרטים אישיים של המשתמש, ייעשה רק לאחר הצהרת הספק במעמד הבדיקה באילו נתונים הוא רוצה להשתמש ומה השימוש שיעשה בהם וקבלת אישור המשרד לכך. הערה בנושא תופיע בשדה הערות/מגבלות באישור.
- 6.3.2 בכל שימוש בחיישנים או ברכיבים נוספים הקשורים למכשיר יש ליידע ולבקש את אישור המשתמש.
- 6.3.3 הגישה לנתונים תיעשה על ידי המשתמש עצמו בצורה יזומה, ולא באופן אוטומטי על ידי האפליקציה.

7. תמיכה מרחוק במשתמשים

- 7.1 ספק שרוצה להפעיל תמיכה מרחוק תוך כדי שימוש בתוכנת שליטה על המשתמשים, צריך לעמוד בדרישות הבאות:
- 7.1.1 ההשתלטות מותנית בהסכמת המשתמש, ואין להתנות שירות באי הסכמה.
- 7.1.2 יש לקבל את הסכמת המשתמש באופן אקטיבי בעת פתיחת ה-Session.
- 7.1.3 יש לקבל את ההסכמה המפורשת של המשתמש לביצוע פעולות מתערבות על גבי מחשב המשתמש.
- 7.1.4 על המשתמש להיות נוכח לאורך כל זמן ההשתלטות ליד המחשב.

- 7.1.5 יש לאפשר למשתמש לנתק את ה-Session לפי שיקול דעתו הבלעדי מצד המחשב שלו.
- 7.1.6 יש לתעד את ההשתלטות במערכת הפניית של הספק.
- 7.1.7 למען הסר ספק, במסגרת הטיפול יש לגשת ליישומים ונתונים הנדרשים לטיפול בלבד. אין לגשת למערכות שאינן באחריות הספק, אין להעתיק/לשלוח קבצים שאינם נדרשים לטיפול בתקלה וללא אישור הלקוח.
- 7.1.8 חל איסור להעביר קבצים ללקוח דרך תוכנת השתלטות.
- 7.1.9 על הספק לבדוק את אמינות תוכנת ההשתלטות.
- 7.1.10 חל איסור להוציא קבצים מתחנת הלקוח המכילים מידע מוגן.
- 7.1.11 אישור הלקוח – יש לתעד בהקלטת שיחה או באישור כתוב את הסכמת המשתמש.
- 7.1.12 יש לוודא שה-Session נסגר בסיום הטיפול.

8. שעת חירום

8.1 תרגילי חירום

- 8.1.1 משרד החינוך נוהג לערוך פעמיים בשנה תרגיל חירום, בדרך כלל בסמוך לתרגיל התגוננות ארצי. ברוב המקרים התרגילים מתקיימים בחודשים פברואר ומאי. מועדי התרגילים מפורסמים בלוח גאנט ארצי המפורסם באתר המשרד.
- 8.1.2 בתרגיל של כלל בתי הספר במדינת ישראל מיישמים למידה מרחוק באמצעות הפורטלים הבית-ספריים ושימוש בספקי תוכן וספרי לימוד דיגיטליים. בזמן התרגיל צפויים עומסים חריגים על המערכות.

8.2 היערכות לזמן חירום / תרגילי חירום

- 8.2.1 הספקים נדרשים להיערך מבעוד מועד כדי לספק מענה כנדרש במערכות מהמערכות המאושרות.
- 8.2.2 על הספק לדאוג בעת תהליך הבדיקה למסור פרטי איש קשר לזמן חירום. אם יש צורך, באחריות הספק לעדכן את המידע מול משרד החינוך.
- 8.2.3 כל ספק פורטל בית-ספרי מאושר ידאג למסמך הדרכה כיצד לשלב במערכת שלו את קישור ה-RSS לשעת חירום.
- 8.2.4 כל ספק ניהול פדגוגי מאושר ידאג למסמך הדרכה כיצד להפיק קישור RSS מהמערכת שלו.

- 8.2.5 . בתקופת זמן חירום/תרגיל על הספק לחסום גישה מחו"ל לאתריו, כאשר החסימה תבוצע מחו"ל.
- 8.3 . פעילות בזמן חירום/תרגיל
- 8.3.1 . הספק ידאג לפעילות תקינה ולזמינות מלאה של המערכות.
- 8.3.2 . על הספק להיות ער לפעילות חשודה באתר ולציוד המחשוב, כגון נפילת שרתים ואירועי אבטחה.
- 8.3.3 . בכל תקלה או אירוע חריג יש לפעול פי סעיף: נוהלי חובה בעת כשל/נפילת מערכת.
- 8.4 . אחרי זמן חירום/תרגיל
- 8.4.1 . על הספק להעביר מידע לגבי עומסי הגלישה במערכת בתקופת זמן החירום ברזולוציה של שעות ביום, לרבות מידע על:
- 8.4.1.1 . Page views
- 8.4.1.2 . Sessions
- 8.4.1.3 . Unique users
- 8.4.1.4 . CPU Utilization
- 8.4.1.5 . Memory Utilization

9. גביית תשלומים

- 9.1 . אם המערכת משמשת לגביית תשלום וסליקת התשלום – על הספק לפעול על פי ההוראות והדרישות של הרשות למשפט, טכנולוגיה ומידע (רמו"ט) בנושא "הנחיות רשם שירותי נתוני אשראי ושירותי מידע על עוסקים" המופיעות באתר שכתובתו:
- <http://www.justice.gov.il/Units/ilita/LawInfo/Hanchayot/HanchayotBetokef/Pages/default.aspx>
- 9.2 . על הספק להעביר למשרד החינוך אישור על עמידה של מערך הסליקה של כרטיסי האשראי בתקן PCI DSS level 1 לפני פתיחת האתר לשימוש המשתמשים.
- 9.3 . על הספק להעביר אישור למשרד החינוך של חברת הסליקה כי אתר הספק עומד בדרישות התקן לפני פתיחת האתר לשימוש המשתמשים.

9.4. חל איסור לשמור באתר הספק את מספרי כרטיסי האשראי או כל מידע רלוונטי אחר אשר אסור לפי תקן PCI DSS.

10. דרישות מספק השירות מחוץ לגבולות מדינת ישראל למידע מוגן וחסוי

- 10.1. בשלב זה תאושר העברת מידע רק למדינות החברות באיחוד האירופי.
- 10.2. יש להבטיח בכתב כי מקבל המידע נוקט אמצעים מספיקים להבטחת פרטיותם של מי שהמידע עליהם, וכי הוא מבטיח שהמידע לא יועבר לאף גורם זולתו, בין אם באותה מדינה ובין אם במדינה אחרת.
- 10.3. על הספק להיות בעל תקן ISO 27001 תקף של השירות בענן או תקן מקביל בנושא ניהול אבטחת מידע.
- 10.4. על הספק לפרט אם השירות בענן עומד בתקני אבטחת מידע בין-לאומיים (כדוגמת זה של Cloud Security Alliance).
- 10.5. התצורה המאושרת לשימוש בעננים היא IaaS - תשתית כשירות. על הספק לבצע מידור של התשתיות הלוגיות (כגון שרתים לוגים, מסדי הנתונים ושירותים נוספים) משירותים של לקוחות אחרים המשתמשים בשירותי ענן. יש לפרט את ארכיטקטורת הרשת התומכת בתקן זה.
- 10.6. על הספק לפרט את התכנית לניהול אבטחת המידע של השירות בענן.
- 10.7. על הספק לפרט את תדירות ביצוע בדיקות חוסן באופן עצמאי וגם על ידי מומחה חיצוני בשכבות התקשורת, מערכת ההפעלה והאפליקציה של השירות בענן.
- 10.8. על הספק לפרט את תדירות ביצוע של סקרי אבטחת מידע באופן עצמאי וגם על ידי מומחה חיצוני בשכבות התקשורת, מערכת ההפעלה והאפליקציה של השירות בענן.
- 10.9. הספק מתחייב כי שימוש בכלים ו/או בשירותים משלימים ו/או חיצוניים לענן יעמדו בדרישות המפורטות במסמך זה.
- 10.10. כל התקשורת לניהול סביבת הענן תתבצע על גבי תווך מוצפן עם הזדהות חזקה.
- 10.11. על ספק שירותי ענן להעביר הודעה מראש לספק על הפסקת שירות – אם ספק הענן נאלץ להפסיק את השירות כתוצאה מצו בית משפט, הפרה של חוק/תקנות או בשל החלטה עסקית/פיננסית.
- 10.12. על ספק שירותי ענן לאפשר העברת המידע והנתונים לספק טרם הפסקת השבתת השירות.

11. תחולה

11.1. תקן זה הוא תקן סופי החל מ-1.12.2013.

11.2. מעת לעת משרד החינוך יעדכן את התקן בהתאם להתפתחויות טכנולוגיות ולצרכים חינוכיים שיעלו.