



משרד החינוך

נספח אבטחת מידע – שרשרת אספקה

גרסה – 1.3

תאריך יישום – 01 אוגוסט, 2018

ניהול שינויים

ניהול שינויים	גרסה	מחבר	תאריך
הוספת התחייבות הקבלן	1.1	שאול בן שושן	
שמות מתחם Domain	1.2	שאול בן שושן	
אבטחת שיחות וועידה	1.3	שאול בן שושן	

מדינת ישראל

משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

נספח אבטחת מידע למיקור חוץ

1. מטרה (I)

מסמך זה כולל אוסף דרישות אבטחת מידע לצורך התקשרות עם הקבלן. עמידה בהוראות מסמך זה הינה תנאי סף להתקשרות עם הקבלן, ועליו לעמוד בדרישות אבטחת מידע של משרד החינוך כפי שיעודכנו מעת לעת.

2. הגדרות (II)

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 הקבלן:** אדם הנמנה על עובדי הקבלן אשר מונה על ידי הקבלן לתפקיד זה ואשר אחראי על אבטחת המידע הנכלל במאגרי המידע המצויים בידי הקבלן ועל יישום ההנחיות המופיעות במסמך זה.

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

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

2.7. **משתמשי מאגר מידע:**

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

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

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

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

2.9. **"התקן נייד"** - מחשב המיועד לשימוש נייד ובכלל זה רדיו טלפון נייד כהגדרתו בחוק התקשורת (בזק ושידורים) התשמ"ב-1982 ואו מצע אחר המשמש לאחסון חומר מחשב;

מדינת ישראל משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

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, והכל ללא רשות כדן;

2.13. **"שלמות מידע"** - זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששנו, נמסרו או הושמדו ללא רשות כדן.

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 בטחון מערכות מחשב. פעולה המתבצעת בזדון או בשוגג.

פעולה זו עלולה לפגוע בזמינות, אמינות וסודיות המידע ו/או בציד 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 הקבלים המאושרת ע"י המשרד.

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

א. פגיעה או הכבדה על ביצוע תוכניות או פעולות כלכליות, מנהליות, חברתיות, משפטיות ואחרות, של המדינה.

ב. גרימת תקלה לעבודת הגופים הציבוריים שמשמעה עיכוב או ייקור תהליכי עבודה, או, הפרעה בביצוע אכיפת החוק.

ג. מידע פנים ארגוני שהנהלת הארגון רוצה לשמור על חשאיותה מול ארגון מתחרה.

3. הנחיות לביצוע (M)

על הקבלן לפרט במענה למכרז את הצעותיו לסעיפים המסומנים ב (S), סעיפים אלו יבדקו כל מנת לוודא שההצעה עונה על דרישות אבטחת מידע.

3.1. סוג 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 הגנה על מידע ולחוק הגנת הפרטיות התשמ"א-1981.

צוות אבטחת מידע סיווג את המידע במערכת כמידע שמור ומוגן.

3.2. סימון המידע (M)

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

מדינת ישראל משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

3.3. התחייבות הקבלן (M)

על הקבלן למלא אחר הוראות נספח זה ואחר יתר הוראות המשרד בכל הנוגע לאבטחת מידע לרבות הוראות אשר יתעדכנו מעת לעת, יישום הוראות המשרד במלואן מהווה תנאי להתקשרות הקבלן עם המשרד, על הקבלן לחתום על ההצהרה בנושא **בסעיף 3.30**.

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 בינלאומי.
- 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 ואז לכל אדם שפרטיו נחשפו מהמערכת.
- הגשת תביעות משפטיות נגד משרד החינוך.
- נזק כלכלי למשרד החינוך ואגף.
- נזק תדמיתי בלתי הפיך למשרד החינוך.
- נזק למידע.

מדינת ישראל משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

3.7. שימוש, אחזקה או ניהול של מאגרי מידע (M)

3.7.1. מלוא המידע המצוי במאגרי המידע של המשרד אשר בידי הקבלן או שיש לספק גישה

אליהם במסגרת ההתקשרות בינו לבין המשרד, הינו בבעלות המשרד על כל המשתמע מכך.

הקבלן מתחייב שכל גישה שלו, או של מי מטעמו, למידע ולמאגר המידע, תתבצע אך ורק

בהתאם להוראות המשרד ולמטרות אשר הוגדרו לו על ידי המשרד במסגרת ההתקשרות.

3.7.2. הקבלן מתחייב שהוא, או מי מטעמו, יקפיד כי כל איסוף מידע או שימוש בו יבוצע אך ורק

בהתאם להוראות החוק והדיון, ועל פי הנחיות המשרד.

3.7.3. הקבלן 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. הקבלן מתחייב למנוע שמירה של נתונים רגישים באופן מקומי אצל משתמשי המערכת.

במקרים חריגים יש לקבל אישור מפורש ובכתב מהמשרד

3.7.5. ככל שהקבלן 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

הרשות להגנת הפרטיות הרלוונטיות, לרבות בנוגע לרישום מאגרים, בהתאם לצורך.

3.7.6. בהתאם להנחיות הממשלה בנושא "אבטחת מידע למעבר לענן ציבורי" המערכת המוצעת

על ידי הקבלן מחייבת אישור וועדת ענן ממשלתית, במידה והקבלן מציע מערכת בענן ציבורי

הקבלן מתחייב לבצע את השינויים והמלצות הוועדה וכן יישום תקנות חוק הגנת הפרטיות

הרלוונטיות טרם הפעלת המערכת.

3.8. (S) בקרה

לצורך בקרה על יישום דרישות אבטחת המידע על הקבלן לקבל אישור של חטיבת אבטחת מידע במשרד

החינוך בשלב התחלת העבודה במערכת, בשלבי שינויים מהותיים במערכת ובשלב הארכת התקשרות.

3.9. זיהוי וניהול סיכונים (M)

3.9.1. (S) על הקבלן לפרט את תוכנית ביצוע ניהול וזיהוי של סיכונים אבטחת מידע בכל שלב

משלבי הפרויקט.

3.9.2. הקבלן מתחייב לפנות למשרד בבקשה לאישור לפני ביצוע שינויים בארכיטקטורת

המערכת, או באופן מתן השירותים. הקבלן מתחייב שלא לבצע שינוי כלשהו ללא אישור

מפורש ובכתב מהמשרד.

3.9.3. הקבלן ראשי להציע בקרות חלופיות לדרישות המפורטות במסמך זה, בקרות אלו יישומו

לאחר אישור בכתב של חטיבת אבטחת מידע

מדינת ישראל

משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

3.10

הצהרה על מחויבות גורם חיצוני בנושא אבטחת מידע (M)

3.10.1 (S) הקבלן יגיש מסמך הצהרה למשרד החינוך בו הוא מצהיר על התחייבותו על ביצוע ההנחיות לשמירת אבטחת המידע כפי שמפורט בהנחיות ובמסמכי משרד החינוך, ובמסמכי המכרז.

3.11

ניהול אבטחת מידע ארגונית (M)

3.11.1 (S) הקבלן מתחייב למנות ממונה אבטחת מידע מטעמו, ואשר יהיה אחראי על אבטחת המידע הנכלל במאגרי המידע המצויים בידי הקבלן וכן על יישום ההנחיות המופיעות במסמך זה, על ממונה אבטחת מידע להיות עם ניסיון של 5 שנים לפחות בתחום אבטחת המידע, יש לצרף למענה את פרטי ממונה אבטחת המידע.

3.11.2 (S) הקבלן יחתום על התחייבות לשמירת סודיות, בנוסח המצורף למכרז, וכן יחתים על התחייבות זו את עובדיו ו/או כל מי מטעמו אשר יהיה בעל גישה למאגר מידע של המשרד או למידע מתוכו במסגרת ההתקשרות.

3.11.3 (S) הקבלן מתחייב להפריד הפרדה מלאה את מאגרי המשרד המצויים בידי מיתר מאגרי המידע שברשותו. זאת באמצעות הפרדה לוגית הכוללת סגמנט מבודד מאחורי חומת אש, יש לפרט את תוכנית ההפרדה ולצרף גם שרטוט רשת.

3.11.4 בכל מקרה שבו לספק התקשרות עם צד שלישי כלשהו אשר יש לה נגיעה עם ההתקשרות בין הקבלן למשרד במסגרת מכרז זה ו/או על יישום ההנחיות המפורטות במסמך זה, הקבלן מתחייב להודיע על כך למשרד ולפעול על פי הנחיותיו וכן ליידיע את הצד השלישי על החובות הנובעות מקיום ההנחיות המפורטות במסמך זה.

3.12

אבטחת המידע במישור משאבי האנוש והעובדים (M)

3.12.1 (S) הקבלן מתחייב כי כל עובדיו ו/או מי מטעמו אשר יהיו בעלי גישה למאגרי המשרד ו/או יועסקו במסגרת התקשרות הקבלן עם המשרד, יהיו בעלי הכשרה מתאימה, בהתאם לנדרש במסמכי המכרז וההתקשרות. בדיקת אימות הרקע של כל מועמד להעסקה כעובד הקבלן, מי מטעמו או משתמש צד שלישי, יעשו ע"י הקבלן כנדרש על פי דין ולפי כללי האתיקה הרלוונטיים, והיקפם יתאים לדרישות המשרד, לסיווג המידע שיהיה נגיש להם ולסיכונים הצפויים.

3.12.2 (S) הקבלן יהיה אחראי כלפי המשרד על כל פעילות עובדיו ו/או מי מטעמו במסגרת ההתקשרות.

3.12.3 (S) הקבלן 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 הקבלן להפחית סיכוני גניבה, הונאה או שימוש לרעה בגישה למידע של המשרד באמצעות נקיטת אמצעי הגנה סבירים ומקובלים (כגון מצלמות אבטחה, תיעוד גישה וכדומה), וזאת מבלי לגרוע מהוראות נספח זה באשר לאבטחה הפיזית והסביבתית.

3.12.4 על הקבלן לבצע הדרכות מודעות אבטחת מידע לעובדיו בתחום העיסוק של העובד בתדירות של אחת לשנה

מדינת ישראל משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

3.12.5. הקבלן מתחייב למנוע מקרים בהם עובדיו ו/או מי מטעמו ינסו לבצע גישות למאגרים אליהם לא קיבלו הרשאה. במקרה בו עובד ו/או מי מטעם הקבלן ניסה בפעם השלישית לבצע גישה למאגר שאינו מורשה גישה אליו, על הקבלן למנוע ממנו כל גישה למאגרי המשרד ולדווח על כך מיידית למשרד.

3.12.6. הקבלן מתחייב כי תפקידים ותחומי אחריות של עובדי הקבלן ו/או מי מטעמו ו/או משתמשי צד שלישי הנוגעים לאבטחה, יוגדרו ויתועדו ע"י הקבלן לפי מדיניות אבטחת המידע של הארגון.

3.12.7. הקבלן מתחייב להודיע באופן מידי למנהל היחידה במשרד החינוך על עזיבה או שינוי תפקיד העובד שיש לו גישה לנתונים, למערכות המידע ו/או מאגרי המידע של המשרד שבידי הקבלן או שיש לקבלן גישה אליהם במסגרת ההתקשרות בינו לבין המשרד

3.13. אבטחה פיזית וסביבתית (M)

3.13.1. הקבלן מתחייב כי הגישה לאזורים שקיים בהם מידע ו/או מאגרי מידע וארונות התקשורת תהייה מתועדת ומבוקרת באופן המאפשר את וידוא זהות האדם הניגש לצידוד הנ"ל הכולל מניעת הכחשה. רשומות הכניסה ישמרו למשך שנתיים ויועברו למשרד החינוך לפי דרישה.

3.13.2. בכל מקרה בו מאגר המידע נמצא ברשות הקבלן, הקבלן מתחייב לתעד הכנסה והוצאה של ציוד אל המתקנים בהם ממוקם המאגר ומהם.

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

3.13.4. אמצעים לבקרת כניסה פיזית: הקבלן 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.

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

3.13.6. עבודה באזורים מאובטחים: הקבלן מתחייב לכתוב וליישם הנחיות לעבודה באזורים מאובטחים.

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

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

3.13.9. תחזוקת ציוד: הקבלן מתחייב לתחזק את הציוד כראוי על מנת להבטיח את זמינותו וכלילותו הרציפות.

מדינת ישראל משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

3.14. מצעי מידע פיזיים (M)

- 3.14.1. על הזכיין ליידע את עובדיו וכל מי שנחשף למידע במסגרת התהליכים שבמשרד על חובת יישום ההנחיות לשמירה על מידע מודפס מצעי מידע פיזיים.
- 3.14.2. באזורי קבלת קהל לא יאוחסן מידע חסוי. חסוי רגיש לא יונח על גבי שולחנות לקבלת קהל.
- 3.14.3. כאשר מצעי מידע פיזיים (כגון: אמצעי אחסון אלקטרוני או ניירת), האוגרים מידע חסוי, אין להשאירם ללא השגחה ולאחר שעות העבודה יש לאחסנם במקום נעול.
- 3.14.4. חל איסור להשאיר פלט המכיל מידע חסוי במדפסות או במכונות צילום, באחריות מדפיס ומצלם המידע לקחת את הפלט במידי
- 3.14.5. מידע חסוי אשר השימוש בו הסתיים, חייב לעבור גריסה או להיות מאוחסן בארכיב מאובטח.

3.15. ניהול תקשורת ותפעול (M)

- 3.15.1. (S) הקבלן מתחייב להגדיר ולעבוד על פי מערך נוהלי עבודה אשר יתנו מענה לכל דרישות משרד החינוך לרבות בנושא אבטחת מידע, **יש לספק דוגמת נהלים.**
- 3.15.2. הקבלן מתחייב שהנהלים ייבדקו על ידו פעם בשנה לפחות ויתוקנו בהתאם להנחיות משרד החינוך.
- 3.15.3. במידה והתגלו ליקויים בעבודת הקבלן, או כתוצאה מגילוי חשיפת אבטחת מידע חדשה, הקבלן מתחייב לעדכן את נוהלי העבודה ולדווח ל משרד החינוך באופן מיידי.

3.16. אבטחה לוגית (M)

- 3.16.1. (S) הקבלן מתחייב ליישם אמצעי אבטחה הולמים שימנעו חדירה מכוונת או מקרית למערכת או למערכות התשתית והתקשורת, **יש לפרט במענה את אמצעי הבקרה שהקבלן מציע.**
- 3.16.2. (S) הקבלן מתחייב לבצע הפרדה בין רשתות המאכלסות את מאגרי המידע של משרד החינוך ליישומים ולכלל הרשתות (סגמנטציה), **יש לצרף למענה את תוכנית ההפרדה ושרטוט רשת.**
- 3.16.3. הקבלן מתחייב שכל אמצעי אבטחת המידע יעברו הקשחות לפי המלצות היצרן.
- 3.16.4. (S) הקבלן מתחייב לעדכן באופן שוטף את המערכות השונות למניעת ניצול פרוצות אבטחת מידע, **יש לצרף למכרז את תוכנית העדכונים.**
- 3.16.5. (S) הקבלן מתחייב שמערכות אבטחת מידע יספקו שרידות מלאה לשמירה על זמינות המערכת, **יש לצרף למענה את תוכנית השרידות והזמינות.**

מדינת ישראל משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

3.17. תיעוד ובקרה (M)

- 3.17.1 (S) הקבלן מתחייב לנהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת על מערכות שניגשות למאגרי מידע של המשרד, יש לצרף למענה את הפתרון לדרישה .
- 3.17.2 הקבלן מתחייב שבכל פניה למערכת ולרשומות במאגר יירשמו כל הנתונים הבאים : זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, והאם הגישה אושרה או נדחתה.
- 3.17.3 הקבלן מתחייב שתיעוד הגישה ישמר בשרתים נפרדים ממאגר המידע.
- 3.17.4 הקבלן מתחייב כי מנגנון הבקרה לא יאפשר, ביטול או שינוי של הפעלתו. מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראי אבטחת מידע מטעם הקבלן ולצוות אבטחת מידע במשרד החינוך.
- 3.17.5 הקבלן מתחייב להעביר למשרד החינוך דיווחים תקופתיים ולפי דרישה בכל הנוגע לאופן ניהול מידע, אשר נמצא בבעלות המשרד.
- 3.17.6 הקבלן מתחייב לדווח באופן מיידי לצוות אבטחת מידע במשרד החינוך בכל מקרה של חשש לדליפת מידע מהמאגר או שימוש חורג מההרשאה שניתנה.
- 3.17.7 הקבלן מתחייב לשמור את נתוני הרישום של מנגנון הבקרה למשך 24 חודשים לפחות.

3.18. ביקורות אבטחת מידע (M)

- 3.18.1 הקבלן מתחייב ליידע את העובדים במאגר בדבר קיומו של מנגנון הבקרה למערכות המאגר והיקף התיעוד המבוצע על ידו.
- 3.18.2 הקבלן מתחייב לאפשר למשרד החינוך לערוך ביקורות באתר המארח את המידע.
- 3.18.3 הקבלן מתחייב לתקן את הליקויים לפי דוח הביקורת של משרד החינוך בתוך פרק הזמן שיקבע על ידי משרד החינוך.

3.19. ניהול המידע (M)

- 3.19.1 הקבלן מתחייב לנהל רשימה של כל נכסי המידע של משרד החינוך שנמצאים ברשותו.
- 3.19.2 הקבלן מתחייב להעביר את רשימת כל נכסי המידע של משרד החינוך שנמצאים ברשותו למינהל תקשוב ומערכות מידע.
- 3.19.3 הקבלן מתחייב להגדיר ולנהל רשימות מורשים לגישה פיזית לנכסי המידע בבעלות משרד החינוך.
- 3.19.4 הקבלן מתחייב שלא להעביר מידע בבעלות משרד החינוך לגורם שלישי ללא אישור בעל המידע במשרד החינוך.
- 3.19.5 הקבלן מתחייב לדווח למשרד החינוך על כל צורך בסילוק ציוד מיחשוב שכולל מידע בבעלות המשרד. סילוק הציוד יהיה אך ורק באישור גורם מוסמך במשרד החינוך.

מדינת ישראל משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

3.19.6. במידה ויש צורך בהשמדת/סילוק מדיה מגנטי כגון, דיסקים, קלטות גיבוי, מדיה נתיקה מכל סוג, פלט נייר וכו' שכולל מידע בבעלות משרד החינוך – הקבלן מתחייב לבער את המידע שבמדיה בהתאם להנחיות ממונה אבטחת מידע במשרד החינוך לאחר גיבוי המידע בהתאם לצורך ולהנחיות המשרד.

3.19.7. הקבלן מתחייב כי בסיום ההתקשרות יתאם עם משרד החינוך את השמדת כל נכסי המידע בבעלות משרד החינוך שנשארו ברשותו.

3.20. ניהול הרשאות גישה (M)

3.20.1 (S) הקבלן 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 ובהתאם להוראות המכרז.

3.20.2. הקבלן מתחייב לדאוג לגישה ממודרת על בסיס הגדרת תפקידים .

3.20.3. הקבלן מתחייב לנהל רישום מעודכן של בעלי התפקידים ושל הגישה המוגדרת לכל תפקיד.

3.20.4. הקבלן מתחייב לגרוע הרשאות לבעלי תפקידים שהסתיים תפקידם או שאין להם צורך במידע אליו קיבלו הרשאה.

3.20.5 (S) הקבלן מתחייב לדאוג לבקורות המתאימות על מנת שלא תבוצע גישה לא מורשית למאגרי המידע, יש לצרף למענה את הפתרון לדרישה

3.20.6. הקבלן מתחייב שהזדהות לניהול הרשת והשירותים הניהוליים מרחוק תבוצע באמצעות רכיב פיסי בנוסף לסיסמא.

3.20.6.1

- חוזק הסיסמא - לפחות 8 תווים בשילוב של ספרות ואותיות
 - מספר ניסיונות שגויים לנעילה - 3 ניסיונות
 - שמירת היסטורית סיסמאות - עד 5 סיסמאות אחורה
 - תדירות החלפת הסיסמא אחת ל-3 חודשים
- 3.20.7.** הקבלן מתחייב לנתק משתמש שהזדהה למערכת מידע לאחר פרק זמן של 10 דקות ללא פעילות .

מדינת ישראל משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

3.21. תיעוד אירועי אבטחה (M)

- 3.21.1 (S) על הקבלן לבצע תיעוד של כל אירוע אשר יש בו משום פגיעה בשלמות סודיות וזמינות המידע, **יש לצרף למענה את הפתרון לדרישה.**
- 3.21.2 כל אירוע אבטחה, יחקר ויבדק ויופק דוח אירוע המתאר את הגורמים לאירוע ואת דרכי הטיפול באירוע. הקבלן יוציא הנחיות לביצוע על מנת להפחית את הסיכוי לאירוע דומה.
- 3.21.3 (S) על הקבלן 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 וכדומה, **יש לצרף למענה דוגמא לדרישה.**

3.22. אבטחת תקשורת (M)

- 3.22.1 הקבלן מתחייב שלא יחבר מערכות /מאגרי מידע למרשתת אלא אם כן קיבל את אישור המשרד לכך.
- 3.22.2 (S) במידה וקיבל הקבלן אישור וחיבר את המערכות ו/או מאגרי המידע לרשת ציבורית או למרשתת, מתחייב הקבלן לנקוט באמצעי ההגנה המתאימים על מנת למנוע נזק, פריצה, זיהום או השחתה של מאגרי המידע, **יש לפרט את הצעת הקבלן להתמודד עם האיומים הנ"ל ולצרף למענה את רשימת הבקורות והאמצעים הנותנים מענה לדרישה.**
- 3.22.3 (S) הקבלן מתחייב שהעברת המידע בתוך רשת התקשורת, ברשת ציבורית או במרשתת תיעשה תוך שימוש בשיטות הצפנה מקובלות.

3.23. שמות מתחם Domain

- 3.23.1 במידה ונדרשת מערכת אינטרנט כתובת האינטרנט תירשם תחת מתחם הכתובות של משרד החינוך XXX.education.gov.il
- 3.23.2 שם הדומיין יקבע על ידי תשתיות משרד החינוך בשילוב ביחידה במשרד
- 3.23.3 תעודה דיגיטלית למתחם הדומיין שיקבע יסופק על ידי משרד החינוך בצורה שלא מאפשרת ייצוא

3.24. אבטחת שיחות וועידה

- במידה ונדרש שיחות וועידה באמצעות מערכות דיגיטליות (כגון Zoom , Teams ו WebEx) המערכות יוגדרו בהתאם להנחיות הבאות:
- 3.24.1 חל איסור להקליט את השיחה
- 3.24.2 אין להשתמש בציט שבמערכות אלו לדו שיח בין המשתתפים
- 3.24.3 כל שיחת ועידה תוגן בסיסמא

מדינת ישראל משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

3.24.4. על מזמין השיחה לאשר כל משתתף שניכנס לחדר השיחה (חדר המתנה)

3.24.5. שיתוף המסך יאושר על ידי מזמין השיחה

3.25. אבטחת תחנות הקצה (M)

חל איסור מוחלט לשמור מידע רגיש בתחנה מרוחקת של המשתמש.

3.26. הגנה על היישום (M)

3.26.1. (S) על מנת לנתר ולהגן על הנתונים שרתי היישום ימוקמו מאחורי חומות אש

אפליקטיבי, יש לפרט את הצעת הקבלן לבקרה נותנת מענה לדרישה.

3.26.2. (S) השרתים ימוקמו מאחורי מערך חומות אש ו IPS למניעת התקפות על היישום.

3.26.3. השרתים יוקשחו לפי הגדרות היצרן כולל מערך בקרה, יש לפרט את הצעת הקבלן

לבקרה נותנת מענה לדרישה.

3.27. התקנים ניידים (M)

3.27.1. הקבלן מתחייב שלא להוציא חלקי מידע אל תווך של התקנים ניידים למעט מדיית גיבוי.

3.27.2. במידה ונדרש מהקבלן לצורך פעילותו לבצע העלאת חלקי מידע לצורך גיבוי, מתחייב

הקבלן לפנות לקבלת אישור צוות אבטחת המידע במשרד החינוך וכן לנקוט באמצעי הגנה

נאותים על מנת להבטיח את שלמות, סודיות וזמינות המידע.

3.27.3. במידה ונדרש מהקבלן לצורך פעילותו לבצע העלאת חלקי מידע לקלטת גיבוי מתחייב

הקבלן לוודא כי אין ערוב של מידע מסיווגים שונים על אותו התקן.

3.27.4. במאגר מידע שניתן להתחבר אליו מרחוק באמצעות המרשתת למטרות ניהול, הקבלן

מתחייב לבצע זיהוי המונע הכחשה של המורשה לגישה מרחוק. לצורך כך יבוצע שימוש ברכיב

פיזי המצוי בשליטתו של המורשה.

3.28. גיבוי, שחזור והתאוששות (M)

3.28.1. הקבלן מתחייב לבצע גיבויים מאובטחים של המידע הנצבר אצלו.

3.28.2. (S) הקבלן מתחייב לאחסן את מדיות הגיבוי בכספת מוגנת אש ומים הנמצאת מחוץ

למתקן המחזיק את מאגרי המידע או שהקבלן יעשה שימוש באמצעים שיבטיחו את שלמות

המידע ויבטיחו את אפשרות שחזור המידע במקרה של אבדן או הרס.

3.28.3. הקבלן מתחייב לבצע שחזורים מדגמיים של המדיות המגבות על תשתיותיו לצורך בדיקת

ההתאוששות.

3.28.4. הקבלן מתחייב כי שחזור אמיתי יבוצע באישור מנהל מאגר המידע.

3.28.5. הקבלן מתחייב כי במידה ובוצע שחזור אמיתי יתועדו כל הליכי השחזור כולל זהותו של

מבצע השחזור.

מדינת ישראל

משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

- 3.28.6. הקבלן מתחייב למנוע עירוב מידע מסיווגים שונים בזמן השחזור.
 3.28.7. לאחר סיום השחזור המדגמי מתחייב הקבלן למחוק את המידע ששוחזר.

3.29. אבטחת מידע אפליקטיבית (M)

במידה והקבלן נדרש לפתח קוד_עליו לפתח בהתאם להנחיות הבאות :

3.29.1. הקבלן מתחייב כי הקוד יפותח לפי כללי האצבע הבאים :

נושא	כלל האצבע
בדיקת קלט ונתונים	• 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 על מנת למנוע Sql Injection
הזדהות	• בצע חלוקה של המערכת לאיזורים פתוחים ואיזורים הדורשים הזדהות • עשה שימוש בסיסמאות חזקות • אל תשמור סיסמאות בצורה גלויה • עשה שימוש בנגנון פג תוקף של סיסמאות ו password policy
הרשאות	• בצע בדיקות הרשאות לפי שייכות המשתמש לתפקידים • הגבל גישה למשאבי מערכת למשתמשים מורשים בלבד
מידע רגיש	• אל תשמור סיסמאות כ clear Text • שמירת מידע רגיש במקומות בטוחים בלבד • עשה שימוש בתשתית Encryption / Decryption סטנדרטית • ואל תפתח מנגנונים עצמיים
ניהול Session	• קצר את משך ה Session ככל שניתן

מדינת ישראל
משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

• 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	ניהול Exceptions
• עשה שימוש במנגנון לוג ו audit מרכזי	Audit & Log
• עשה שימוש בנגנון Url Autorization לדפים ומחיצות	Asp.Net
• עשה שימוש ב command parameters על מנת למנוע Sql Injection	Dal / פניה לבסיס הנתונים

3.29.2. (S) על הקבלן לפרט את המתודולוגיה ותהליכי אבטחת המידע בפיתוח של מערכות המידע הנדרשות למכרז

1.1.1. בדיקת חדירות - הקבלן מתחייב לבצע בדיקות חוסן באמצעות חברה חיצונית בלתי תלויה המתמחה בבדיקות חוסן אפליקטיביות ותשתיות למערכות המשמשות לאחסון, עיבוד והתשתיות התומכות במכרז זה. בדיקות אלה יבוצעו לא על נתוני אמת של המערכת המקורית. במידה וקיים 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. על הקבלן לתקן את הליקויים שהתגלו בבדיקת חדירות טרם עליית המערכת לייצור.

3.30. אי עמידה בהוראות אבטחת מידע בנספח אבטחת מידע

3.30.1.1. המשרד רשאי לקנוס את הקבלן על אי יישום האמור בסעיף 3.8 בעניין קבלת אישור מנהל אבטחת המידע 1,000 ₪ לכל יום שהקבלן לא קיבל אישור ממנהל אבטחת מידע של משרד החינוך על עמידה בדרישות.

3.30.1.2. המשרד רשאי לקנוס את הקבלן על אי יישום האמור בנספח זה עד - 1,000 ₪ ליום לכל סעיף שלא יושם.

3.30.1.3. על בקבלן לחתום על הצהרה הבאה:

מדינת ישראל
משרד החינוך מנהל מערכות מידע



צוות אבטחת מידע

אני _____, ת.ז. _____, תפקיד _____ מחברת _____ מתחייב לא

להפעיל את המערכות הממוחשבות שלטובת המכרז ו\או לאסוף לעבד או להעביר מידע ללא אישור של מנהל אבטחת מידע וסייבר של משרד החינוך.

אני מאשר כי ידוע לי שבמידה והפעילויות הממוחשבות יופעלו על ידי החברה ללא אישור מנהל אבטחת מידע וסייבר של משרד החינוך המשרד רשאי לקנוס את החברה בהתאם לסעיף 3.30 " **אי עמידה בהוראות אבטחת מידע** **בנספח אבטחת מידע** " במכרז זה.

חתימה + חותמת

_____ החברה _____ תאריך