מדינת ישראל
משרד החינוך

נספח ג' (v1.6)

פרק אבטחת מידע וסייבר

1. מטרה

מסמך זה כולל אוסף דרישות אבטחת המידע וסייבר של משרד החינוך (להלן "המשרד") לצורך התקשרות עם המציע. עמידה בהוראות מסמך זה הינה תנאי סף להתקשרות המשרד עם המציע. על המציע לעמוד בדרישות אבטחת מידע של המשרד כפי שיעודכנו מעת לעת כמפורסם באתר משרד החינוך.

2. הגדרות

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

2.2. מידע חסוי – מידע פנים ארגוני שהארגון רוצה לשמור על חשאיותו, ופגיעה בזמינותו בשלמותו באמינותו, בסודיותו או בשרידותו עלולה לגרום לתקלות כגון פגיעה או הכבדה על ביצוע תכניות, תהליכי עבודה, פעולות כלכליות, מנהליות, חברתיות, משפטיות ואחרות, של המשרד.

2.3. מאגר מידע – אוסף נתוני מידע המוחזק באמצעי מגנטי או אופטי (ובכלל זה מחשב ו/או מחשוב ענן) ומיועד לעיבוד ממוחשב.

2.4. הממונה על אבטחת המידע והסייבר מטעם המציע – גורם הנמנה על עובדי המציע אשר הוגדר כממונה לתפקיד זה ואחראי על אבטחת המידע והסייבר הנכלל במאגרי המידע המצויים בידי המציע ועל יישום ההנחיות המופיעות במסמך זה.

2.5. הממונה על אבטחת המידע והסייבר במשרד – גורם שמונה לתפקיד זה מטעם המשרד שאחראי על אבטחת המידע והסייבר במשרד, ואחראי על מתן הנחיות אבטחת מידע וסייבר.

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

2.7. תקיפת סייבר – אירוע אבטחה (Incident) שמטרתו לעבור או לעקוף את אמצעי האבטחה או הבקרה בהם המציע או המשרד עושים שימוש, או לגרום לשיבוש בשירותים הניתנים על ידי המציע, או לנצל חולשה קיימת בניסיון לגרום לנזק, אובדן, דלף, שינוי, שימוש, חשיפה לא מורשית או גישה למידע של המשרד.

2.8. משתמשי מאגר מידע

2.8.1. כל בעל תפקיד מטעם המציע, הנדרש מתוקף תפקידו להשתמש במידע אשר נצבר במאגרי המידע של המשרד המצויים אצל המציע, או שיש למציע גישה אליהם.

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

2.8.3. מערכות משיקות (צד שלישי) העושות שימוש במידע הנכלל במאגרי המידע של משרד והמצויים בידי המציע.

2.9. אבטחה פיזית – האמצעים הפיזיים הנדרשים להגנה על ציוד המחשוב, לגישה למידע של משרד ולשרידות המערכות הממוחשבות המכילות את מאגרי המידע.

2.10. התקן נייד – הינו אמצעי אחסון אלקטרוני נייד שניתן לחבר למחשב באמצעים פיזיים או אלחוטיים. כולל Disk on key מסוג USB, כוננים קשיחים חיצוניים, כרטיסי זיכרון, מדיה אופטית, סמארטפונים, טאבלטים וכו'.

2.11. סיווג מידע - הקניית הגדרת רגישות למידע, בהתבסס על העקרונות שהותוו על ידי המשרד לנושא אבטחת מידע וסייבר במשרד.

2.12. נזק למידע – פגיעה בסודיות, בשלמות וזמינות המידע בבעלותו של משרד.

2.13. אבטחת מידע – הגנה על סודיות, שלמות וזמינות המידע בבעלותו של משרד. הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין ;

2.14. שלמות מידע – זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין.

2.15. סודיות המידע – חשיפת המידע לגורמים לא מורשים.

2.16. זמינות המידע – שמירה על נגישות למידע באופן רציף.

2.17. אירוע במ"מ – אירוע בטחון מערכות מחשב. פעולה המתבצעת על ידי עובד בזדון או בשוגג.

2.18. מיקור חוץ – השימוש בשירותי מיקור חוץ משמעו הוצאת פעילות מחוץ לארגון, או ביצוע פעילות על ידי גורם צד שלישי שאינו עובד בארגון, המבצע פעולות ותהליכים המבוצעים בדרך כלל על ידי הארגון.

3. דרישות אבטחת מידע, סייבר ופרטיות

הנחיות למענה המציע

א. על המציע לעמוד <u>בכל</u> דרישות אבטחת מידע, סייבר ופרטיות המופיעות בפרק זה.

ב. ככל ונדרשות הבהרות, על המציע לרכז רשימת שאלות וחומרים רלוונטיים בהתאם למבנה פרק האבטחה ולהעבירם למשרד **<u>בשלב שאלות ההבהרה בלבד</u>** לקבלת מענה.

ג. על המציע **לסמן** ☒ **בכל סעיף** בעמודת אישור המציע, המהווה אישור לכך שהמציע **קרא, הבין, מקובל עליו ויפעל בהתאם לדרישות פרק זה.**

ד. בסעיפים בהם המציע נדרש לצרף צרופות או פירוט נוסף **על המציע לספק את כל המסמכים הרלוונטיים.**

ה. הספק 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.

3.1 כללי		
3.1.1	המשרד רואה חשיבות רבה במימוש שיטתי ויעיל של היבטי אבטחת המידע, ובכלל זה היבטים הקשורים להגנה על מידע ולעמידה בחוק הגנת הפרטיות התשמ"א-1981.	
3.1.2	על המציע לפרט ולהציג למשרד, ככל שיידרש לעשות זאת, את האמצעים בהם הוא נוקט לשם שמירה על אבטחת המידע לרבות מסמכים רלוונטיים.	
3.1.3	**על המציע להיות בעל הסמכה בתוקף לתקן ISO27001.**	
סעיף	**דרישה**	**אישור המציע**
3.2 שמירה על מידע		
3.2.1	המשרד הינו הבעלים הבלעדיים של המידע, לרבות המידע נשוא מכרז זה המאוחסן בסביבת המציע. המציע יעשה שימוש במידע אך ורק למטרת היענות מלאה לדרישות המכרז.	☐
3.2.2	המציע הינו הגורם האחראי לכל חשיפה, פגיעה, נזק, מניעת גישה, אבדן של מידע רגיש או חשיפה של מידע לצד שלישי אשר עלול לגרום למשרד, וכן לצדדי ג' נזקים.	☐
3.2.3	המציע מחויב לשמור על המידע של המשרד, לרבות מידע רגיש ו/או חסוי, בהתאם לסטנדרטים מקובלים בשוק.	☐

3.2.4	המציע מתחייב שהוא, או מי מטעמו, לא יעביר מידע רגיש ו/או חסוי, או חלק ממידע רגיש ו/או חסוי, אשר בידיו או שיש לו גישה אליהם, לגורם צד שלישי כלשהו ללא אישור מפורש ובכתב מאת המשרד.	☐
3.2.5	חל איסור מוחלט להעברת מידע של המשרד באמצעות התקן נייד.	☐
3.2.6	במידה וקיים צורך ייעודי בשימוש בהתקן נייד להעברת מידע רגיש/חסוי יש לקבל על כך אישור מראש ובכתב מהמשרד.	☐
3.2.7	המציע מתחייב כי מידע רגיש לרבות מידע פרטי מזוהה יאוחסן אך ורק בתשתית מאובטחת וכי העברת המידע אל ומתשתית זו יעשה באופן מאובטח. על תשתית זו ועל תהליכי שמירת והעברת הנתונים לעמוד בדרישות תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017, חוק הגנת הפרטיות, התשמ"א 1981.	☐
3.2.8	העברה ושיתוף מידע רגיש ו/או חסוי בין המציע למשרד **<u>לא יועברו במייל</u>** ויבוצעו על ידי מנגנון מאובטח ומוצפן להעברת קבצים (בכספת או בענן) כפי שיאושר ע"י המשרד.	☐
3.2.9	ככל שהמציע יחזיק במידע פרטי מזוהה יש לסמן כל פלט בכיתוב: "מכיל מידע רגיש לפי חוק הגנת הפרטיות - המוסר שלא כדין עובר עבירה".	☐
3.2.10	ככל שהמציע נדרש להפעיל גורם צד שלישי לצורך ביצוע הפעילות במסגרת המכרז. יש להודיע למשרד אודות ההתקשרות עם גורם צד שלישי ובאחריות המציע לוודא כי הגורם צד שלישי מחויב לעמידה בהנחיות המשרד.	☐
3.2.11	המציע מתחייב למנות ממונה על אבטחת המידע מטעמו, אשר יהיה אחראי על הטיפול במידע של המשרד המצוי בידו, וכן על יישום ההנחיות המופיעות במסמך זה.	☐
3.2.12	המציע מחויב להגן על המידע של המשרד כל עוד המידע מצוי אצלו, גם לאחר תום תקופת המכרז.	☐
3.3 אבטחת מידע בתשתיות הטכנולוגיות של המציע		
3.3.1	המציע יציג למשרד, ככל שיידרש, את האמצעים בהם הוא נוקט לשם אבטחת המידע.	☐
3.3.2	המציע מתחייב ליישם אמצעי אבטחה הולמים שימנעו חדירה מכוונת או מקרית למערכות, שרתים, מחשבים ותשתיות התקשורת של המציע לרבות יישום האמצעים הבאים:	☐
3.3.2.1	חומת אש (Firewall) ואמצעי גלישה מאובטחת להגנה בפני אתרים זדוניים ומתחזים (פישינג) בין מחשבי ומערכות המציע לרשת האינטרנט.	☐
3.3.2.2	אמצעי הגנה מתקדמים לנקודות קצה בפני וירוסים, כופר, קוד זדוני ועוד, כגון: EDR/XDR בכל תחנות העבודה, השרתים, והמחשבים הניידים בסביבת המציע.	☐

3.3.2.3	מערכת דואר אלקטרוני מאובטחת הכוללת הגנה מפני וירוסים ופישינג.	☐
3.3.2.4	העלאת קבצים למערכות ותשתיות טכנולוגיות של המציע תעבור תהליך הלבנה לסריקת ווירוסים ונוזקות שונות.	☐
3.3.2.5	כל אמצעי אבטחת המידע בסביבת המציע יעברו הקשחות לפי המלצות היצרן(Best Practice).	☐
3.3.2.6	עדכוני טלאי תוכנה ואבטחה תדירים לתוכנות, מערכות הפעלה והאפליקציות בסביבת המציע.	☐
3.3.2.7	הזדהות חזקה למחשבים ולשרתים של המציע תתבצע באמצעות סיסמאות מורכבות (לפחות 10 תווים) ו/או מנגנון הזדהות חזק אחר כגון אימות רב-גורמי (MFA), הזדהות ביומטרית וכדומה.	☐
3.3.2.8	על המציע לנטר את מערכותיו בהיבטי סייבר על ידי מערך ניטור SOC (Security Operation Center) 24/7 (24 שעות ביממה, 365 ימים בשנה).	☐
3.3.2.9	על כל מחשב נייד של המציע המחזיק מידע בנושא המכרז להיות מוגן על ידי מערכת הצפנת דיסק (Full Disk Encryption).	☐
3.3.2.10	אין להשאיר התקנים ניידים כגון מחשב נייד, כונן חיצוני וכו' האוגרים מידע רגיש ו/או חסוי, ללא השגחה. כמו כן, לאחר שעות העבודה יש לוודא אחסונם במקום נעול.	☐
3.3.3	המציע נדרש לבצע בדיקות חוסן תקופתיות באופן עצמאי או על ידי מומחה חיצוני לתשתיות וליישומים הטכנולוגיים הקיימים בסביבת המציע.	☐
3.3.4	המציע נדרש לבצע סקרי אבטחת מידע תקופתיים באופן עצמאי או על ידי מומחה חיצוני לתשתיות וליישומים הטכנולוגיים הקיימים בסביבת המציע.	☐
3.4 אבטחת המערכות אשר באמצעותן המציע מבצע את עבודתו		
3.4.1	המציע מתחייב לעמוד בדרישות הבאות:	
3.4.1.1	יישום מנגנון הזדהות משתמשים הכולל MFA (Multi Factor Authentication).	☐
3.4.1.2	מידור הרשאות לפי עקרון 'הצורך לדעת' (Need to Know) המאפשר למשתמש המורשה בלבד גישה למידע במערכת בה מנוהלים מסמכי המשרד ובהתאם לצורך למילוי תפקידו.	☐
3.4.1.3	גישה למערכות המידע ו/או מאגרי המידע תהיה ממודרת ברמת זיהוי משתמש ולא תורשה גישה מעבר לנדרש (Least Privilege) לצורך מילוי התפקיד.	☐
3.4.1.4	המציע מתחייב לבצע סקירה ותיקוף הרשאות באופן תקופתי.	☐
3.5 שימוש במערכות ומחשוב ענן		

3.5.1	על ספק שירותי הענן בהם המציע עושה שימוש לצורך מתן השירותים למשרד להיות בעל תקן ISO 27001.	☐
3.5.2	המידע של המשרד יישמר במלואו בגבולות מדינת ישראל או לחילופין על גבי תשתית ענן מאובטח תחת מדינות החברות באיחוד האירופי, ובשירות אחסון מאובטח העומד בתקינת אבטחת מידע וסטנדרטים בינלאומיים לרבות ISO27001, SOC2, GDPR, CSA.	☐
3.5.3	על המציע לבצע מידור של התשתיות הלוגיות (כגון שרתים לוגים, מסדי הנתונים ושירותים נוספים) משירותים של לקוחות אחרים המשתמשים בשרותי הענן.	☐
3.5.4	על המציע לנהל תכנית ניהול אבטחת מידע לסביבת שירותי הענן שלו.	☐
3.5.5	המציע מתחייב כי שימוש בכלים ו/או בשירותים משלימים ו/או חיצוניים לענן יעמדו בדרישות המפורטות במסמך זה.	☐
3.5.6	כל התקשורת לניהול סביבת הענן תתבצע על גבי תווך מוצפן (In Transit) בפרוטוקול מאובטח התומך בפרוטוקול TLS1.3 או TLS1.2 בלבד.	☐
3.5.7	כל המידע של המשרד הנשמר בסביבת הענן של המציע יישמר באופן מוצפן במנוחה (At Rest) בהצפנה בתקן AES-256 ומעלה.	☐
3.5.8	יובהר כי במידה ונדרש לשמור מידע רגיש/חסוי בענן על המציע לקבל על כך אישור בכתב מהמשרד.	☐
3.6 גיבויים ומניעת אובדן מידע		
3.6.1	המציע מתחייב לעשות כל שנדרש למניעת אובדן מידע במסגרת ההתקשרות, באמצעות ביצוע גיבויים באופן סדיר ומאובטח. כמו כן, יש לבצע בדיקות שחזור מגיבוי באופן תקופתי.	☐
3.6.2	הגיבויים יישמרו באופן מאובטח ובמקום נפרד מהמערכת/תשתית בהם שמור המידע של המשרד.	☐
3.6.3	המציע מתחייב לבצע שחזורים מדגמיים של המדיות המגבות על תשתיותיו לצורך בדיקת התאוששות. לאחר סיום השחזור המדגמי מתחייב המציע למחוק את המידע ששוחזר.	☐
3.6.4	שחזור אמיתי יבוצע אך ורק באישור המשרד. כל הליכי השחזור יתועדו כולל זהותו של מבצע השחזור.	☐
3.7 תיעוד ובקרה		
3.7.1	המציע מתחייב לנהל מנגנון תיעוד אוטומטי שיאפשר בקרה וביקורת עבור כל גישה למידע במערכת לרבות זהות המשתמש, התאריך והשעה של ניסיון הגישה, סוג הגישה, והאם הגישה אושרה או נדחתה.	☐
3.7.2	המציע מתחייב לדווח באופן מידי לצוות אבטחת מידע במשרד בכל מקרה של חשש לדליפת מידע של המשרד מהמאגר וממערכות המציע או כל שימוש החורג מההרשאה שניתנה.	☐

3.8 אבטחת ההון האנושי		
3.8.1	המציע מתחייב כי כל עובדיו ו/או מי מטעמו אשר יהיו בעלי גישה למידע של המשרד ו/או יועסקו במסגרת התקשרות המציע עם המשרד, יהיו בעלי הכשרה מתאימה, בהתאם לנדרש במסמכי המכרז וההתקשרות. בדיקת אימות הרקע של כל מועמד להעסקה כעובד המציע, מי מטעמו או משתמש צד שלישי, יעשו ע"י המציע כנדרש על פי דין ולפי כללי האתיקה הרלוונטיים, והיקפם יתאים לדרישות המשרד, לסיווג המידע שיהיה נגיש להם ולסיכונים הצפויים.	☐
3.8.2	המציע יהיה אחראי כלפי המשרד על כל פעילות עובדיו ו/או מי מטעמו במסגרת ההתקשרות.	☐
3.8.3	המציע נדרש להכין הוראות להתמודדות עם אירועי במ"מ (ראה הגדרות). על המציע להעביר למשרד את דוח האירוע בתוך 72 שעות מתחילת האירוע. למשרד שמורה הזכות לזמן את המציע לתחקור האירוע והפקת לקחים.	☐
3.8.4	המציע 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.	☐
3.8.5	המציע מתחייב לנקוט באמצעי הגנה סבירים ומקובלים (כגון מצלמות אבטחה, בקרת כניסה, תיעוד גישה וכדומה) להפחתת סיכוני גניבה, הונאה או שימוש לרעה בגישה למאגרי המידע והיישומים של המשרד.	☐
3.8.6	על המציע לבצע הדרכות מודעות אבטחת מידע לעובדיו בתחום העיסוק של העובד בתדירות של אחת לשנה.	☐
3.8.7	המציע מתחייב כי תפקידים ותחומי אחריות של עובדי המציע ו/או מי מטעמו ו/או משתמשי צד שלישי הנוגעים לאבטחה, יוגדרו ויתועדו ע"י המציע לפי מדיניות אבטחת המידע של הארגון.	☐
3.8.8	המציע מתחייב להודיע באופן מידיי למשרד על עזיבה או שינוי תפקיד העובד שיש לו גישה למידע ו\או מאגרי המידע של המשרד שבידי המציע או שיש למציע גישה אליהם במסגרת ההתקשרות בינו לבין המשרד.	☐
3.9 אבטחת שיחות וועידה		
3.9.1	במידה והמציע נדרש לקיים שיחות וועידה באמצעות מערכות דיגיטליות (כגון: Zoom, Teams, Google Meet, WebEx וכדומה) המערכות יוגדרו בהתאם להנחיות הבאות:	
3.9.1.1	ככלל, אין להקליט מפגשים. במקרים חריגים בהם נדרשת הקלטה היא תעשה באישור המשרד ולאחר יידוע המשתתפים	☐
3.9.1.2	כברירת מחדל יש לחסום את האפשרות לכתוב בצ'אט. במידה ועולה צורך להשתמש בצ'אט יש להנחות את המשתתפים שלא לשתף מידע פרטי או רגיש.	☐

3.9.1.3	במקרה של אירוע חשוד או אירוע אבטחתי, יש לסיים את המפגש באופן מידי או לחילופין לנתק את המשתתפים החשודים מהשיחה.	☐
3.9.1.4	יש לאשר פרטנית כל משתתף שניכנס לחדר השיחה (כניסה ראשונית לחדר המתנה).	☐
	3.10 שימוש בכלי AI ובינה מלאכותית יוצרת (Generative AI)	
3.10.1	המציע מתחייב שלא להעלות או לשתף עם כלי בינה מלאכותית כל מידע או חומרים הקשורים לפעילות המציע במסגרת מתן שירותיו למשרד.	☐
3.10.2	המציע מתחייב שלא להעלות או לשתף עם כלי בינה מלאכותית כל מידע או חומרים שקיבל מהמשרד לרבות טקסט, קוד, תמונות, קבצים, אודיו וכדומה.	☐
	3.11 חובת דיווח	
3.11.1	המציע מתחייב להודיע למשרד, בהקדם האפשרי ובתוך 8 שעות, במהלך כל שעות היממה, וללא שיהוי, ובפרק זמן שלא יעלה על 12 שעות על כל אירוע אבטחה, בדגש על אירוע אשר מסכן מידע, מערכות או תהליכים של המשרד או עלול להשפיע על יכולתו לעמוד בהתחייבויותיו נשוא מכרז זה, ובפרט יודיע למשרד על האירועים הבאים:	☐
3.11.1.1	אירוע אבטחה או תקיפת סייבר אשר הביאו לדלף מידע הקשור למשרד או לשיבושו של מידע או קוד תוכנה.	☐
3.11.1.2	אירוע אבטחה או ניסיון תקיפת סייבר אשר עלול להביא לפגיעה במידע של המשרד, במערכות המסופקות לו או בקוד המשמש אותו.	☐
3.11.1.3	ניסיון להחדרת קוד זדוני למערכות המציע בהן נשמר מידע של המשרד.	☐
3.11.1.4	אירוע אבטחה או ניסיון תקיפת סייבר אשר מטרתו לאסוף מידע על המשרד.	☐
3.11.1.5	חולשה או חשיפה משמעותיים שאותרו במערכות באמצעותן המציע מספק שירות למשרד.	☐
3.11.2	במקרה כאמור, על המציע להודיע למשרד על התרחשות האירוע ועל כל פרט נוסף ביחס לאירוע זה לרבות: תיאור כללי של האירוע, אופן התרחשותו, סקירת היסטוריית האירוע, יעדי התקיפה, המערכות אשר נפגעו, המידע אשר זלג או נפגע, ניתוח דרכי התקיפה, החולשות ששימשו את התקיפה וכל מידע רלוונטי אחר לצורך ניתוח האירוע.	☐
	3.12 ביקורת תקופתית	
3.12.1	המציע מתחייב לאפשר למשרד לערוך מעת לעת ביקורת תקופתית אודות עמידת המציע בדרישות אבטחת המידע, הפרטיות והסייבר במסגרת אספקת השירותים למשרד. ביקורת זו תתבצע במתקני המציע, בהודעה מראש של	☐

	לפחות 7 ימי עבודה, או בדרך של בקשת דוחות ודיווחים על אופן עמידת המציע בדרישות המכרז לאבטחת מידע וסייבר. על המציע להעביר את הדוחות והדיווחים בהתאם ללוח הזמנים שיוגדר על ידי המשרד.	
3.12.2	המציע מתחייב לתקן את הליקויים שיעלו בביקורת אבטחת מידע שתבוצע על ידי המשרד (או גורם מטעמו) בתוך פרק זמן סביר שייקבע על ידי המשרד.	☐
3.12.3	המציע מתחייב למלא פעם בשנה שאלון הצהרה עצמית, אשר יישלח באופן מקוון לתיקוף רמת אבטחת המידע. יש לענות על השאלון תוך פרק זמן של עד 14 יום ממועד קבלת השאלון.	☐
3.13 סיום התקשרות		
3.13.1	עם סיום ההתקשרות, המציע ימסור למשרד גיבוי מלא, בפורמט סטנדרטי של כל המידע המאוחסן, כל מצע מידע נייד (כגון מדיה אופטית, קלטת, כרטיס זיכרון, FlashDrive וכו') קוד המקור שנכתב (כולל תיעוד והסברים לקוד המקור, הפניות לקוד מקור Open Source שנעשה בו שימוש, באגים ופגיעויות אבטחת מידע ידועות) וכן כל מקור וההעתק של הדוחות והרישומים הסופיים שהופקו לשם מתן מענה למכרז. מיד לאחר אישור משרד על תקינות המידע שהתקבל, ובכפוף להוראת הדין, ישמיד המציע את כלל החומרים שיוותרו בידיו ויבצע מחיקה מלאה (Wipe) של כלל נתוני משרד שברשותו.	☐

4. אבטחת המערכת המוצעת –דרישות ושאלות בנושא אבטחת מידע, סייבר ופרטיות עבור שירותי <u>תוכנה</u>

סעיף	דרישה	אישור המציע
4.1 אימות ובקרת גישה		
4.1.1	הכניסה למערכת נדרשת לתמוך במנגנון הזדהות אחודה (SSO) לממשקי הניהול והמשתמש.	☐
4.1.2	המערכת נדרשת לתמוך באופן מובנה בעבודה עם SAML 2.0 ו- ADFS.	☐
4.1.3	ההזדהות למערכת תהיה בעלת יכולת התממשקות לאחד ממנגנוני ההזדהות של משרד החינוך ו/או תתמוך בכל מנגנון אימות רב גורמי MFA (Multi Factor Authentication) חלופי באישור המשרד.	☐
4.1.4	המערכת נדרשת לתמוך בהחלת מדיניות סיסמאות למשתמשי המערכת (לרבות משתמשים מקומיים), אשר תכלול הגדרה של פרמטרים כגון: אורך מינימלי, מורכבות, תוקף (משך חיי סיסמה מקסימלי ומינימלי), היסטוריית סיסמאות, אכיפת MFA, הסיסמה תישמר בתצורה מוצפנת, נעילה לאחר מספר ניסיונות שגויים וכדומה.	☐

4.1.5	המערכת נדרשת לתמוך בהגבלת זמני פעילות ה- Session כך שמשתמש אשר יחרוג מזמן הפעילות שיוגדר ינותק (Session expired).	☐
4.1.6	המערכת נדרשת לתמוך בניתוק אוטומטי של משתמש לאחר חוסר פעילות שיוגדר במערכת (No-activity timeout).	☐
4.1.7	על המערכת לכלול באופן מובנה מנגנוני ניהול הרשאות ובקרת גישה מבוססת תפקידים כגון RBAC/ABAC.	☐
4.1.8	על כל ממשק בין המערכת המוצעת למערכות המשרד להשתמש בפרוטוקול מאובטח התומך בפרוטוקול TLS1.3 או TLS1.2 בלבד. תוך כדי שימוש בתעודות עם מפתח ציבורי ופרטי אשר מונפקות על ידי CA מאושר.	☐
4.1.9	המציע מתחייב לנהל רישום מעודכן של בעלי התפקידים ושל הגישה המוגדרת לכל תפקיד.	☐
	4.2 הגנה על המידע	
4.2.1	המערכת המוצעת נדרשת לתמוך כברירת מחדל בהצפנה במנוחה (at rest) לכל נתוני התוכן הנשמרים במערכת בעלי היבטי פרטיות.	☐
4.2.2	המערכת המוצעת נדרשת לתמוך בתקשורת מוצפנת בתווך (in transit) אל מול כל רכיבי המערכת הפנימיים והחיצוניים.	☐
4.2.3	המציע נדרש להגביל את הרשאות הגישה לממשקי הניהול ולתשתיות המערכת למינימום הנדרש (Least Privilege) ולמשתמשים מורשים בלבד.	☐
4.2.4	אין להעביר בסיסי נתונים מסביבת הייצור לסביבת הפיתוח ללא התממה או מיסוך נתונים רגישים.	☐
4.2.5	אין לאחסון מפתחות הצפנה בקוד (Hardcoded) על המפתחות להיות מאוחסנים במיקום חיצוני למערכת.	☐
4.2.6	העלאת הקבצים למערכת תתבצע תוך כדי בדיקת הקבצים מפני וירוסים ונוזקות והלבנתם (באמצעות מערכת ICAP או פתרון אחר שיאושר בכתב ע"י המשרד).	☐
	4.3 גישת תמיכה	
4.3.1	המציע יספק תמיכה, ליווי, הטמעה ומענה לתקלות עבור המערכת המוצעת, באופן טלפוני או באופן מקוון או בהתאם לצורך באופן פיזי באתר המשרד.	☐
4.3.2	תמיכה מרחוק למערכות המשרד תתבצע מסביבה ייעודית שיגדיר המשרד או על ידי שימוש בתוכנת שליטה מאובטחת באישור והסכמה מפורשת ובכתב של המשרד.	☐
4.3.3	במסגרת הטיפול המציע יספק תמיכה ליישומים ונתונים הנדרשים לטיפול בלבד. אין לגשת למערכות שאינן באחריות המציע, אין להעתיק/לשלוח קבצים שאינם נדרשים לטיפול בתקלה וללא אישור המשרד.	☐
4.3.4	המציע יבצע את פעולת התמיכה אך ורק בליווי עובד המשרד מצוות היישום אשר יהיה נוכח לאורך כל זמן ההשתלטות ליד המחשב. המציע מחויב לוודא שה-Session נסגר בסיום הטיפול.	☐

4.4 פיתוח קוד וניהול תצורה		
4.4.1	המערכת המוצעת תתבסס על שפת קוד (סגור/פתוח) מודרני ומהימן, בגרסה עדכנית, מתוחזקת ונתמכת באופן פעיל.	☐
4.4.2	כל רכיבי המערכת המוצעת לרבות שרתים, מערכות הפעלה, בסיסי נתונים, אפליקציה, רכיב ענן ועוד יוקשחו לפי המלצות יצרן או תקן NIST.	☐
4.4.3	המציע נדרש לבצע בקרה על הכנסת תוכנה ממקור חיצוני (כגון חבילות קוד פתוח, ספריות קוד, או מוצרי צד שלישי) לרבות סריקת חולשות/פגיעויות אבטחה מוכרות.	☐
4.4.4	הקוד ייסרק באמצעי SAST (Static Application Security Testing) ו-DAST (Dynamic Application Security Testing). ליקויי תוכנה ואבטחה אשר יופיעו בדוח הסריקה יתוקנו בטרם העלאתם לסביבת הייצור.	☐
4.4.5	המציע נדרש ליישם תהליכי פיתוח מאובטח (SSDLC) עבור המערכת המוצעת לאורך כל מחזור החיים של המערכת.	☐
4.4.6	המערכת המוצעת נדרשת לעמוד בדרישות OWASP Top 10 - Application Security Risks.	☐
4.4.7	המערכת המוצעת נדרשת לעמוד בדרישות OWASP Top 10 - CI/CD Security Risks.	☐
4.4.8	הספק נדרש לבצע מבדקי חדירה (PT) אפליקטיביים וסקרי קוד (Code Review) תקופתיים אחת לשנה לכל רכיבי המערכת המוצעת וזאת באמצעות חברה המוסמכת לנושא.	☐
4.4.9	המציע מתחייב לטפל בכל הממצאים/ליקויים ובהתאם להנחיות שיועברו לו על ידי המשרד ולתקן כל הנדרש לצמצום הסיכון ופערי האבטחה. לאחר תיקון הממצאים יש לערוך בדיקת אבטחת מידע חוזרת.	☐
4.5 דרישות לאפליקציית בתצורת מובייל		
4.5.1	הנגשת המערכת בתצורת אפליקציית מובייל תתבצע על ידי מפיצים רשמיים כגון Google Play ו-Apple App Store, או בהתאם להנחיות אבטחת מידע של המפיצים הרשמיים ובכפוף לאישור המשרד.	☐
4.5.2	האפליקציה לא תשמור מידע מוגן או חסוי במכשיר ללא הצפנת הנתונים.	☐
4.5.3	האפליקציה תאפשר למשתמשים למחוק את כל הנתונים הקשורים אליה באופן פשוט וברור.	☐
4.5.4	האפליקציה יכולה להשתמש בזיכרון המכשיר לשמירת מידע כל עוד הוא אינו מאפשר לאפליקציות אחרות גישה למידע, ובתנאי שהמידע מוצפן, לרבות נתוני הזדהות.	☐
4.5.5	התקשורת בין האפליקציה לשרת ההזדהות צריכה להיות מוצפנת ומאובטחת.	☐

4.5.6	הגישה לאפליקציה המכילה מידע מוגן מחייבת הזדהות חזקה כגון אימות רב-גורמי (MFA), הזדהות ביומטרית וכדומה.	☐
4.5.7	גישת האפליקציה לנתונים השמורים במכשיר, כגון אנשי קשר, תמונות ופרטים אישיים של המשתמש, ייעשה רק לאחר הצהרת המציע במעמד הבדיקה באילו נתונים הוא רוצה להשתמש ומה השימוש שייעשה בהם ובכפוף לקבלת אישור מהמשרד.	☐
	4.6 תחזוקת סביבת הפיתוח	
4.6.1	יש לבצע הפרדה מוחלטת בין סביבת הייצור לסביבת הפיתוח. כמו כן, יש לבצע הפרדה בין סביבות הפיתוח לסביבות אחרות.	☐
4.6.2	יש לנהל גרסאות פיתוח בשרת מרכזי (Control Source) לדוגמה: TFS או SVN, או שירות GIT.	☐
4.6.3	אין לאפשר לתכניתנים גישה לבסיסי נתונים בסביבת הייצור.	☐
	4.7 ניטור וחקירה	
4.7.1	על המערכת לכלול רישום ותיעוד מסודר ורציף ללוג (Log) של כל גישה, שינוי הגדרות ופעילות משתמשים וקבצים במערכת.	☐
4.7.2	קבצי הלוג במערכת יהיו מוגנים מפני גישה (צפייה, שינוי, מחיקה) של משתמשי ומנהלי המערכת ו/או גורמים לא מורשים.	☐
4.7.3	על המערכת לכלול תמיכה בהעברה ושידור קבצי לוג ואירועים למערכות ניטור אבטחתי כגון SIEM ו- SOAR. בפורמטים מקובלים כגון syslog.	☐
	4.8 דרישות למערכת המוצעת בתצורת ענן	
4.8.1	המערכת נדרשת לפעול מאזור ענן ציבורי (Region) של אחד מספקי הענן זוכי מכרז נימבוס (Google GCP או Amazon Web Services) בשטח הטריטוריאלי של מדינת ישראל (להלן: "**האזור הישראלי**"), או לחילופין על בסיס אזור ענן של אחד מספקים אלו בתחומי האיחוד האירופי, בכפוף לאישור המשרד.	☐
4.8.2	אחסון המערכת המוצעת יבוצע על גבי תשתית ענן פרטי וירטואלי (VPC) ייעודי למשרד ומבודל ברמת Tenant.	☐
4.8.3	הגישה למערכת המוצעת בענן תבוצע תחת מנגנוני בקרת גישה לרשת (NACLs) ותוגבל לכתובת IP מאושרת שיגדיר המשרד.	☐
4.8.4	כל נתוני המשרד הקיימים במערכת המאוחסנת בענן יישמרו אך ורק בתוך אזור הענן (Region) הספציפי שבו מאוחסנת המערכת המוצעת.	☐
4.8.5	על סביבת הענן בה מתארחת המערכת המוצעת לכלול ניטור אבטחתי והגנות מתקדמות לרבות DDoS, IDS/IPS, FW, WAF, IAM לסינון והגנה בפני מתקפות על המערכת.	☐

4.8.6	על המערכת לאפשר המשכיות עבודה בעת תקלה מערכתית או אסון, תוך פריסתה בלפחות שני Availability Zones באותו אזור ענן (Region).	☐

4.9 מסמכים נדרשים מטעם המציע	
4.9.1	**<u>על המציע לצרף את כל המסמכים הבאים</u>:**
4.9.1.1	הסמכת ISO27001 של המציע.
4.9.1.2	הסמכות, תקנים וסטנדרטים נוספים בהיבטי אבטחת מידע ופרטיות בהם מוסמך המציע כגון SOC2 / HIPPA / PCI.
4.9.1.3	מיפוי סוגי המידע הקיימים במערכת.
4.9.1.4	פירוט תהליכים ארגוניים ואמצעי אבטחה לצמצום סיכונים והתמודדות עם איומי סייבר ושרשרת אספקה.
4.9.1.5	טופס הערכת עובדים ובדיקות מהימנות.
4.9.1.6	שרטוטי ארכיטקטורה של המערכת המוצעת ומיפוי ממשקים.
4.9.1.7	פירוט המתודולוגיה ותהליכי אבטחת המידע במחזור חיי הפיתוח של המערכת המוצעת.
4.9.1.8	דו״ח עדכני של מבדק חדירה (PT) וסקר קוד תקין של המערכת המוצעת.
4.9.1.9	נהלי גיבוי, שחזור ו – DR.
4.9.1.10	נוהל זיהוי ותגובה לאירועי סייבר (Incident Response).
4.9.1.11	יש לצרף למענה את תוכנית התמודדות בפני סיכונים במסגרת הפרויקט.

הצהרת המציע
אני מאשר/ת בזאת כי הדרישות המפורטות בפרק זה מיושמות במלואן. שם המציע/ת _____ חתימה: _____ תאריך _____
תצהיר של ממונה אבטחת מידע של המציע בעניין אבטחת מידע

אני הח"מ _____ ת"ז מס' _____ לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי/ה לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

1. הנני משמש ממונה אבטחת מידע בחברת _____ שהגישה הצעה למכרז מספר [ ] (שם המציע)

2. בתוקף תפקידי, הנני מצהיר/ה כי:

א. קראתי את ההוראות המופיעות במכרז כולל נספח X.

ב. הדרישות המופיעות בהוראות הנ"ל מובנות לי והנני מתחייב להיערך בהתאם ולפעול על פיהם במסגרת מכרז זה.

ג. החברה לא הפרה בעבר הוראות הנוגעות לאבטחת מידע או ככל שאירעו בעבר הפרות של הוראות הנוגעות לאבטחת מידע, הללו תוקנו עד למועד הגשת ההצעה.

3. הנני מצהיר כי זה שמי, זו חתימתי וכי תוכן הצהרתי אמת.

חתימת המצהיר

תאריך	שם מלא של ממונה אבטחת מידע של המציע	חתימה של ממונה אבטחת מידע וחותמת של המציע

אני החתום/מה מטה, עורך/כת דין _____, מאשרת/ת בזה כי ביום _____ הופיע/ה בפני מר/גב' _____ שזהיתיו/ה לפי תעודת זהות מס' _____ המוכר/ת לי אישית ולאחר שהזהרתיו/ה כי עליו /ה לומר את האמת בלבד ואת האמת כולה וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, אישר/ה נכונות הצהרתו/ה דלעיל וחתם/ה עליה בפני.

תאריך	שם מלא של עו"ד, מ.ר.	חתימה וחותמת

תצהיר של המנהל הכללי של המציע בעניין אבטחת מידע

אני הח"מ _____ ת"ז מס' _____ לאחר שהוזהרתי כי עלי לומר את האמת וכי אהיה צפוי/ה לעונשים הקבועים בחוק אם לא אעשה כן, מצהיר/ה בזה כדלקמן:

1. הנני משמש כמנהל הכללי בחברת _____ שהגישה הצעה למכרז מספר [ ] (שם המציע)

2. בתוקף תפקידי, הנני מצהיר/ה כי:

א. קראתי את ההוראות המופיעות במכרז כולל נספח X.

ב. הדרישות המופיעות בהוראות הנ"ל מובנות לי והנני מתחייב להיערך בהתאם ולפעול על פיהם במסגרת מכרז זה.

ג. החברה לא הפרה בעבר הוראות הנוגעות לאבטחת מידע.

3. הנני מצהיר כי זה שמי, זו חתימתי וכי תוכן הצהרתי אמת או ככל שאירעו בעבר הפרות של הוראות הנוגעות לאבטחת מידע, הללו תוקנו עד למועד הגשת ההצעה.

חתימת המצהיר

תאריך	שם מלא של מנהל הכללי של המציע	חתימה של מנהל הכללי וחותמת של המציע

אני החתום/מה מטה, עורך/כת דין _____, מאשרת/ת בזה כי ביום _____ הופיע/ה בפני מר/גב' _____ שזהיתיו/ה לפי תעודת זהות מס' _____ המוכר/ת לי אישית ולאחר שהזהרתיו/ה כי עליו /ה לומר את האמת בלבד ואת האמת כולה וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם לא יעשה/תעשה כן, אישר/ה נכונות הצהרתו/ה דלעיל וחתם/ה עליה בפני.

תאריך	שם מלא של עו"ד, מ.ר.	חתימה וחותמת

נספח הצהרת סודיות

<u>הצהרה וכתב התחייבות בדבר שמירה על סודיות וקיום הוראות חוק הגנת הפרטיות</u>

אל: חטיבת אבטחת מידע וסייבר / משרד החינוך
מאת: _____
שם מלא _____ מספר זהות_____
נייד _____ כתובת _____

אני, הח"מ מצהיר ומתחייב בזאת כלפי משרד החינוך כדלהלן:
הואיל ולצורך עבודתי עבור משרד החינוך עלי לקבל נתונים, מסמכים, רשימות, תוכניות, מידע רגיש, מידע רפואי רגיש, תרשימים, צילומים, על אמצעים מגנטיים, חומר מצולם, מודפס וכו' (להלן – **מידע**) וגישה אל מידע ומאגרי מידע השייכים למשרד החינוך ולקוחותיו;
והואיל והובהר לי, כי חובה עליי לשמור בסוד מוחלט כל מידע אליו אחשף במישרין או בעקיפין במסגרת עבודתי במשרד החינוך וכי שמירת הסודיות הכרחית מטעמים לביטחון המדינה וכי גילוי מידע רגיש או מסווג, לכל גורם אשר אינו מורשה לקבלו מתוקף תפקידו, עלול לפגוע בביטחון המדינה ומהווה עבירה על החוק;
והואיל וידוע לי כי על פי חוק הגנת הפרטיות התשמ"א-1981, והתקנות שהותקנו לפיו, ועל פי חוק העונשין, תשל"ז 1977 -בכלל ועל פי סעיף 113 א לחוק זה בפרט מוטלות עלי ועל כל מי שפועל מטעמי חובת סודיות לגבי כל המידע והנתונים שהגיעו ויגיעו לידיעתי ולידיעת הפועל מטעמי, אשר הפרתן מהווה עבירה פלילית אשר עונש בצידה;

אשר על כן, הנני מצהיר ומתחייב כדלקמן:

1. לשמור בסודיות ולהגן על כל מידע אשר יגיע לידי, לרשותי או לידיעתי, במסגרת עבודתי עבור משרד החינוך מפני חשיפתו בפני גורמים שאינם מוסמכים לקבלו.
2. להימנע מכל גילוי, פרסום, העתקה ו/או העברה בדרך כלשהי ו/או פרסום של מידע כאמור, שהגיע לידי באופן ישיר או עקיף בקשר לעבודתי עבור משרד החינוך, ולא למסור דבר לאדם שאינו מוסמך באשר למידע זה בין בכתב, בין בעל-פה, בין ברמז ובין במפורש, או בכל דרך אחרת, הן בתקופת העסקתי במשרד החינוך והן לאחר סיום העסקתי.
3. לנקוט באמצעי זהירות ובאבטחת מידע כלפי המידע, על מנת למנוע את הוצאת המידע מרשותי והעברתו לאחר שלא הוסמך לקבלו
4. להשתמש במידע שהגיע לידי אך ורק למטרה או להנחיה או להוראה שניתנה לי על ידי הגורמים המוסמכים במשרד החינוך.
5. ידוע לי, כי הפרת התחייבויותיי כאמור עלולה להוות עבירה לפי סימן ה' בפרק ו' לחוק העונשין התשל"ו-1977. הוראות סימן ה' בפרק ו' לחוק העונשין והוראות חוק הגנת הפרטיות התשמ"א-1981 הובאו לידיעתי בטרם חתימתי על הצהרה זו.
6. התחייבותי לשמירת סודיות אינה מוגבלת זמן
7. .בחתימתי אני מאשר כי קראתי את ההנחיות המפורטות לעיל, הבנתי את תוכנן ואני מתחייב למלא אותן.

שם מלא _____ תפקיד _____

חתימה _____ תאריך _____

נחתם בנוכחות _____ תפקיד _____