מדינת ישראל
משרד החינוך

תקן אבטחת מידע וסייבר

1. מטרה

מסמך זה כולל אוסף דרישות אבטחת המידע וסייבר של משרד החינוך (להלן "המשרד"). על המערכת המוצעת לעמוד בדרישות אבטחת מידע של המשרד כפי שיעודכנו מעת לעת כמפורסם באתר משרד החינוך.

2. הגדרות

2.1. מידע מוגן – מתייחס וכולל את כל סוגי המידע המפורטים בהגדרות להלן:

2.1.1. **מידע אישי** – נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי: מי שניתן לזהותו במאמץ סביר, במישרין או בעקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון, או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי כהגדרתו בחוק הגנת הפרטיות התשמ"א -1981.

2.1.2. **מידע בעל רגישות מיוחדת** – מצב בריאותי, מידע גנטי, מזהה ביומטרי, מוצא, עבר פלילי, דעות פוליטיות, אמונות דתיות, השקפת עולם, הערכת אישיות מטעם גורם מקצועי שכדרך עיסוק מחווה דעתו על אישיותו של אדם, או שנערכה באמצעי שמיועד לביצוע הערכה של מאפייני אישיות מהותיים, ובכלל זה קווי אופי, יכולת שכלית ויכולת תפקוד בעבודה או בלימודים, נתוני מיקום ונתוני תעבורה אודות מיקומו של אדם שיש בהם כדי ללמוד על מידע, נתוני שכר, פעילות פיננסית, מידע איש שחלה עליו חובת סודיות, מידע אחר שקבע שר המשפטים כהגדרתו בחוק הגנת הפרטיות התשמ"א -1981.

2.1.3. **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.

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

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

2.4. 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.

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

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

2.7. משתמשי מאגר מידע

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

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

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

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

2.9. 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'.

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

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

2.12. אבטחת מידע – הגנה על סודיות, שלמות וזמינות המידע בבעלותו של משרד. הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל 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 בטחון מערכות מחשב. פעולה המתבצעת על ידי עובד בזדון או בשוגג.

2.17. 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

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 ותקנותיו.	
3.1.2	על הספק לפרט ולהציג למשרד, ככל שיידרש לעשות זאת, את האמצעים בהם הוא נוקט לשם שמירה על אבטחת המידע לרבות מסמכים רלוונטיים.	
3.1.3	ככלל, המוצרים המסופקים לבתי הספר נדרשים להיות מבוססי ממשק אינטרנטי, ללא צורך בהתקנה מקומית.	
3.1.4	**על הספק להיות בעל הסמכה בתוקף לתקן ISO27001.**	
סעיף	**דרישה**	**אישור המציע**
3.2 שמירה על מידע		
3.2.1	המשרד הינו הבעלים הבלעדיים של המידע הנוצר על הפלטפורמה אותה מספק הספק.	☐
3.2.2	הספק הינו הגורם האחראי לכל חשיפה, פגיעה, נזק, מניעת גישה, אבדן של מידע מוגן או חשיפה של מידע לצד שלישי אשר עלול לגרום למשרד, וכן לצדדי ג' נזקים.	☐
3.2.3	הספק מחויב לשמור על המידע המוגן של המשרד בהתאם לסטנדרטים מקובלים בשוק.	☐
3.2.4	הספק מתחייב שהוא, או מי מטעמו, לא יעביר מידע מוגן, או חלק ממנו, 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	הספק מתחייב כי מידע מוגן יאוחסן אך ורק בתשתית מאובטחת וכי העברת המידע אל ומתשתית זו יעשה באופן מאובטח. על תשתית זו ועל תהליכי	☐

	שמירת והעברת הנתונים לעמוד בדרישות חוק הגנת הפרטיות התשמ"א 1981 ותקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.	
3.2.7	העברה ושיתוף מוגבלין הספק למשרד **<u>לא יועברו במייל</u>** ויבוצעו על ידי מנגנון מאובטח ומוצפן להעברת קבצים (בכספת או בענן) כפי שיאושר ע"י המשרד.	☐
3.2.8	ככל שהספק יחזיק במידע אישי יש לסמן כל פלט בכיתוב: "מכיל מידע אישי לפי חוק הגנת הפרטיות - המוסר שלא כדין עובר עבירה".	☐
3.2.9	ככל שהספק נדרש להפעיל גורם צד שלישי לצורך ביצוע הפעילות. יש להודיע למשרד אודות ההתקשרות עם גורם צד שלישי ובאחריות הספק לוודא כי הגורם צד שלישי מחויב לעמידה בהנחיות המשרד.	☐
3.2.10	הספק מתחייב למנות ממונה על אבטחת המידע מטעמו, אשר יהיה אחראי על הטיפול במידע של המשרד המצוי בידו, וכן על יישום ההנחיות המופיעות במסמך זה.	☐
3.2.11	הספק מחויב להגן על המידע של המשרד כל עוד המידע מצוי אצלו.	☐
3.3 אבטחת מידע בתשתיות הטכנולוגיות של הספק		
3.3.1	הספק יציג למשרד, ככל שיידרש, את האמצעים בהם הוא נוקט לשם אבטחת המידע.	☐
3.3.2	הספק מתחייב ליישם אמצעי אבטחה הולמים, שימנעו חדירה מכוונת או מקרית למערכות, שרתים, מחשבים ותשתיות התקשורת של הספק 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 EDR/XDR בפני וירוסים, כופר, קוד זדוני ועוד. בכל תחנות העבודה, השרתים, והמחשבים הניידים בסביבת המציע.	☐
3.3.2.3	מערכת דואר אלקטרוני מאובטחת מטעם החברה (לא מייל פרטי) הכוללת הגנה מפני וירוסים ופישינג.	☐
3.3.2.4	העלאת קבצים למערכות ותשתיות טכנולוגיות של השרתים המארחים מטעם הספק תעבור סריקת וירוסים ונוזקות שונות. ספקי מערכות ניהול פדגוגי, ניהול שעות, ניהול כספים ומערכות המחזיקות מידע רגיש/חסוי, נדרשים ליישם בנוסף מערכת הלבנה.	☐
3.3.2.5	ספקי מערכות ניהול פדגוגי, ניהול שעות, ניהול כספים ומערכות המחזיקות מידע רגיש/חסוי, נדרשים ליישם בנוסף מערכת הלבנה.	☐
3.3.2.6	כל אמצעי אבטחת המידע בסביבת הספק יעברו הקשחות לפי המלצות היצרן(Best Practice).	☐
3.3.2.7	יש לבצע עדכוני טלאי תוכנה ואבטחה תדירים לתוכנות, מערכות הפעלה והאפליקציות בסביבת הספק.	☐

3.3.2.8	הזדהות חזקה למחשבים ולשרתים של הספק תתבצע באמצעות סיסמאות מורכבות (לפחות 10 תווים) ו/או מנגנון הזדהות חזק אחר כגון אימות רב-גורמי (MFA), הזדהות ביומטרית וכדומה.	☐
3.3.2.9	ספקי מערכות ניהול פדגוגי, ניהול שעות, ניהול כספים ומערכות המחזיקות מידע רגיש/חסוי, נדרשים לנטר את מערכותיהם בהיבטי סייבר על ידי מערך ניטור SOC (Security Operation Center) 24/7 (24 שעות ביממה, 365 ימים בשנה).	☐
3.3.2.10	על כל מחשב נייד של הספק המחזיק מידע משרדי רגיש/חסוי להיות מוגן על ידי מערכת הצפנת דיסק (Full Disk Encryption).	☐
3.3.2.11	אין להשאיר התקנים ניידים כגון מחשב נייד, כונן חיצוני וכו' האוגרים מידע מוגן, ללא השגחה. כמו כן, לאחר שעות העבודה יש לוודא אחסונם במקום נעול.	☐
3.3.3	הספק נדרש לבצע בדיקות חדירות (PT) אחת לשנה על ידי חברה בע"מ המתמחה במתן שירותי בדיקות חדירות וסקרי חוסן ולתקן את הליקויים בהתאם.	☐
3.3.4	שרתי האירוח של המערכת/אפליקציה מטעם הספק יהיו חסומים לגלישה אל האינטרנט.	☐
3.3.5	הספק נדרש לבצע סקרי סיכוני אבטחת מידע תקופתיים באופן עצמאי או על ידי מומחה חיצוני לתשתיות וליישומים הטכנולוגיים הקיימים בסביבת הספק ולתקן את הליקויים בהתאם.	☐
3.4 אבטחת המערכות אשר באמצעותן הספק מבצע את עבודתו		
3.4.1	הספק מתחייב לעמוד בדרישות הבאות:	
3.4.1.1	יישום מנגנון הזדהות משתמשים הכולל MFA (Multi Factor Authentication).	☐
3.4.1.2	המערכת נדרשת לכלול מנגנון ההזדהות חזקה עבור מנהלי המערכת (Admins).	
3.4.1.3	מידור הרשאות לפי עקרון 'הצורך לדעת' (Need to Know) המאפשר למשתמש המורשה בלבד גישה למידע במערכת ובהתאם לצורך למילוי תפקידו.	☐
3.4.1.4	גישה למערכות המידע ו/או מאגרי המידע תהיה ממודרת ברמת זיהוי משתמש ולא תורשה גישה מעבר לנדרש (Least Privilege) לצורך מילוי התפקיד.	☐
3.4.1.5	הספק מתחייב לבצע סקירה ותיקוף הרשאות אחת לשנה לכל הפחות.	☐
3.5 שימוש במערכות ומחשוב ענן		

3.5.1	על ספק שירותי הענן בהם הספק עושה שימוש לצורך מתן השירותים למשרד להיות בעל תקן ISO 27001 ו- SOC2.	☐
3.5.2	המידע של המשרד יישמר במלואו בגבולות מדינת ישראל בשירות אחסון מאובטח העומד בתקינת אבטחת מידע וסטנדרטים בינלאומיים לרבות ISO27001, SOC2, GDPR, CSA.	☐
3.5.3	על הספק לבצע מידור של התשתיות הלוגיות (כגון שרתים לוגים, מסדי הנתונים ושירותים נוספים) משירותים של לקוחות אחרים המשתמשים בשרותי הענן.	☐
3.5.4	על הספק לגבש תכנית ניהול אבטחת מידע לסביבת שירותי הענן שלו.	☐
3.5.5	הספק 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 מוגנבענן על הספק לקבל על כך אישור בכתב מהמשרד.	☐
	3.6 גיבויים ומניעת אובדן מידע	
3.6.1	הספק מתחייב לעשות כל שנדרש למניעת אובדן מידע, באמצעות ביצוע גיבויים באופן סדיר ומאובטח. כמו כן, יש לבצע בדיקות שחזור מגיבוי באופן תקופתי.	☐
3.6.2	הגיבויים יישמרו באופן מאובטח ומוצפן ובמיקום נפרד מהמערכת/תשתית.	☐
3.6.3	הספק מתחייב לבצע שחזורים מדגמיים של המדיות המגבות על תשתיותיו לצורך בדיקת התאוששות. לאחר סיום השחזור המדגמי מתחייב הספק למחוק את המידע ששוחזר.	☐
	3.7 תיעוד ובקרה	
3.7.1	הספק 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	הספק מתחייב לדווח באופן מידי לצוות אבטחת מידע במשרד בכל מקרה של חשש לדליפת מידע וממערכות הספק או כל שימוש החורג מההרשאה שניתנה.	☐
	3.8 אבטחת ההון האנושי	

3.8.1	הספק מתחייב כי כל עובדיו ו/או מי מטעמו אשר יהיו בעלי גישה למידע של המשרד ו/או יועסקו במסגרת התקשרות הספק עם המשרד, יהיו בעלי הכשרה מתאימה. בדיקת אימות הרקע של כל מועמד להעסקה כעובד הספק, מי מטעמו או משתמש צד שלישי, יעשו ע"י הספק כנדרש על פי דין ולפי כללי האתיקה הרלוונטיים.	☐
3.8.2	הספק יהיה אחראי כלפי המשרד על כל פעילות עובדיו ו/או מי מטעמו במסגרת ההתקשרות.	☐
3.8.3	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 ולהחתימם על התחייבות לשמירה על הסודיות.	☐
3.8.4	הספק 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.	☐
3.8.5	על הספק לבצע הדרכות מודעות אבטחת מידע לעובדיו בתחום העיסוק של העובד בתדירות של אחת לשנה.	☐
3.8.6	הספק מתחייב כי תפקידים ותחומי אחריות של עובדי הספק ו/או מי מטעמו ו/או משתמשי צד שלישי הנוגעים לאבטחה, יוגדרו ויתועדו ע"י הספק לפי מדיניות אבטחת המידע של הארגון.	☐
3.8.7	במערכות העושות שימוש בצילום והקלטה של תלמידים על הספק לקבל אישור פרטני מהמשרד. השימוש במערכת על ידי בית הספר יהיה מותנה באישור הורים.	☐
3.9 שימוש בכלי AI ובינה מלאכותית יוצרת (Generative AI)		
3.9.1	הספק מתחייב שלא להעלות או לשתף עם כלי בינה מלאכותית כל מידע או חומרים הקשורים לפעילות הספק במסגרת מתן שירותיו למשרד.	☐
3.9.2	הספק מתחייב שלא להעלות או לשתף עם כלי בינה מלאכותית כל מידע או חומרים שקיבל מהמשרד לרבות טקסט, קוד, תמונות, קבצים, אודיו וכדומה.	☐
3.9.3	על הספק לקבל אישור בכתב מהמשרד על שימוש, שילוב או הטמעת יכולות בינה מלאכותית במערכות וכלי תוכן דיגיטליים.	☐
3.10 חובת דיווח		
3.10.1	הספק 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, ובפרט יודיע למשרד על האירועים הבאים:	☐

3.10.1.1	אירוע אבטחה או תקיפת סייבר אשר הביאו לדלף מידע הקשור למשרד או לשיבושו של מידע או קוד תוכנה.	☐
3.10.1.2	אירוע אבטחה או ניסיון תקיפת סייבר אשר עלול להביא לפגיעה במידע של המשרד, במערכות המסופקות לו או בקוד המשמש אותו.	☐
3.10.1.3	ניסיון להחדרת קוד זדוני למערכות הספק בהן נשמר מידע של המשרד.	☐
3.10.1.4	אירוע אבטחה או ניסיון תקיפת סייבר אשר מטרתו לאסוף מידע על המשרד.	☐
3.10.1.5	חולשה או חשיפה משמעותיים שאותרו במערכות באמצעותן הספק מספק שירות למשרד.	☐
3.10.2	במקרה כאמור, על הספק 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.	☐
3.11 ביקורת תקופתית		
3.11.1	הספק מתחייב לאפשר למשרד לערוך מעת לעת ביקורת תקופתית אודות עמידת הספק בדרישות אבטחת המידע, הפרטיות והסייבר במסגרת אספקת השירותים למשרד. ייתכן שביקורת זו תתבצע במתקני הספק, בהודעה מראש של לפחות 7 ימי עבודה, או בדרך של בקשת דוחות ודיווחים על אופן עמידת הספק בדרישות לאבטחת מידע וסייבר. על הספק להעביר את הדוחות והדיווחים בהתאם ללוח הזמנים שיוגדר על ידי המשרד.	☐
3.11.2	הספק מתחייב לתקן את הליקויים שיעלו בביקורת אבטחת מידע שתבוצע על ידי המשרד (או גורם מטעמו) בתוך פרק זמן סביר שייקבע על ידי המשרד.	☐
3.11.3	הספק מתחייב למלא פעם בשנה שאלון הצהרה עצמית, אשר יישלח באופן מקוון לתיקוף רמת אבטחת המידע.	☐
3.12 סיום התקשרות		
3.12.1	עם סיום ההתקשרות, הספק 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 תוכנה

סעיף	דרישה	אישור המציע
4.1 אימות ובקרת גישה		
4.1.1	ההזדהות למערכת תהיה באמצעות מנגנון ההזדהות האחידה של משרד החינוך. כל מנגנון אימות רב גורמי MFA (Multi Factor Authentication) אחר דורש אישור בכתב מטעם המשרד.	☐
4.1.2	הכניסה למערכת נדרשת לתמוך במנגנון הזדהות אחודה (SSO) לממשקי הניהול והמשתמש.	☐
4.1.3	המערכת נדרשת לתמוך באופן מובנה בעבודה עם SAML 2.0 או OpenID .	☐
4.1.4	המערכת נדרשת לתמוך במנגנון הזדהות מקומי כגיבוי במקרה של תקלה במנגנון ההזדהות הראשי, כולל החלת מדיניות סיסמאות למשתמשים (כולל משתמשים מקומיים), מנגנון איפוס סיסמה, שמירת היסטוריית סיסמאות והגדרת דרישות לסיסמאות מורכבות.	☐
4.1.5	המערכת נדרשת לכלול מנגנון ההזדהות חזקה עבור מנהלי המערכת (Admins).	☐
4.1.6	המערכת נדרשת לתמוך בהגבלת זמני פעילות ה- Session כך שמשתמש אשר יחרוג מזמן הפעילות שיוגדר ינותק הניתוק ייקבע לפי רגישות המידע במערכת (מערכת עם מידע ציבורי - לאחר רצף עבודה של 12 שעות ; מערכת עם מידע פרטי/רגיש – לאחר רצף עבודה של 8 שעות).	☐
4.1.7	המערכת נדרשת לתמוך בניתוק אוטומטי של משתמש לאחר חוסר פעילות שיוגדר במערכת (No-activity timeout). משך הזמן עד לניתוק אוטומטי לאחר חוסר פעילות יקבע לפי רגישות המידע במערכת (מידע ציבורי – שעה ; מידע פרטי/רגיש – חצי שעה).	☐
4.1.8	על המערכת לכלול באופן מובנה מנגנוני ניהול הרשאות ובקרת גישה מבוססת תפקידים כגון RBAC/ABAC.	☐
4.1.9	על כל ממשק בין מערכת הספק 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.	☐
4.1.10	הספק מתחייב לנהל רישום מעודכן של בעלי התפקידים ושל הגישה המוגדרת לכל תפקיד.	☐
4.2 הגנה על המידע		

4.2.1	המערכת נדרשת לתמוך כברירת מחדל בהצפנה במנוחה (at rest) לכל נתוני התוכן הנשמרים במערכת בעלי היבטי פרטיות.	☐
4.2.2	המערכת נדרשת לתמוך בתקשורת מוצפנת בתווך (in transit) אל מול כל רכיבי המערכת הפנימיים והחיצוניים.	☐
4.2.3	הספק 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 וסינון קבצים לפי סיומות בעלי פוטנציאל לסיכון.	☐
	4.3 גישת תמיכה	
4.3.1	הספק יספק תמיכה, ליווי, הטמעה ומענה לתקלות עבור המערכת, באופן טלפוני או באופן מקוון.	☐
	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	הספק 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	הספק 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.	☐

4.4.9	הספק מתחייב לטפל בכל הממצאים/ליקויים שיעלו בבדיקות, ולתקן את 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 בהסכמת המשתמש. במעמד הבדיקה, הספק יגדיר אילו נתונים הוא צריך ומה השימוש שייעשה בהם.	☐
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 למפתחים 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	מערכות ניהול פדגוגי ומערכות ניהול כספים יכללו תמיכה בהעברה ושידור קבצי לוג ואירועים למערכות ניטור אבטחתי כגון SIEM ו- SOAR. בפורמטים מקובלים כגון syslog.	☐

4.8 דרישות למערכת הספק 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 ספקים אחרים בשטח הטריטוריאלי של מדינת ישראל, ובכפוף לאישור המשרד.	☐
4.8.2	אחסון המערכת והמידע הקיים בה יבוצע על גבי תשתית ענן פרטי וירטואלי (VPC) ייעודי למשרד ומבודל ברמת Tenant.	☐
4.8.3	כל נתוני המשרד הקיימים במערכת המאוחסנת בענן יישמרו אך ורק בתוך אזור הענן (Region) הספציפי שבו מאוחסנת המערכת.	☐
4.8.4	על סביבת הענן בה מתארחת המערכת לכלול ניטור אבטחתי והגנות מתקדמות לרבות IAM ,WAF, FW, IDS/IPS, DDoS לסינון והגנה בפני מתקפות על המערכת.	☐
4.8.5	על המערכת לאפשר המשכיות עבודה בעת תקלה מערכתית או אסון, תוך פריסתה בלפחות שני Availability Zones באותו אזור ענן (Region).	☐
4.9 דרישות למערכת בינה מלאכותית (AI)		
4.9.1	המציע מתחייב לוודא שמערכת הבינה המלאכותית מבוססת על מודל מהימן ואינה חורגת מגבולות הגזרה והמטרות שהוגדרו לה.	☐
4.9.2	המערכת תבצע שימוש במודל בינה מלאכותית מהימן וברישוי בלבד.	☐
4.9.3	יש לבצע בדיקות קלט/פלט צ׳אט מול הזרקות קוד, הטיות, חריגות, ותכנים בלתי הולמים.	☐
4.9.4	על המערכת לתמוך בניטור באופן רציף של פלט הצ׳אט לטובת זיהוי חריגות ותכנים לא מורשים.	☐
4.9.5	על המערכת לכלול הצפנת כל שיחות הצ׳אט עם מערכת ה-AI (פרומפטים ותגובות), כולל שיחות היסטוריות, בכל תצורות אחסון זמני וקבוע, באמצעות מנגנוני הצפנה מודרניים.	☐
4.9.6	על המערכת לתמוך ביכולת מחיקת חשבונות משתמשים על ידי המשרד באופן מידי ועצמאי.	☐
4.9.7	על המערכת לכלול יכולת לביצוע מחיקה מלאה, הכוללת את כל השיחות הצ׳אט (כולל היסטוריה) עם מערכת ה- AI.	☐
4.9.8	על המערכת לתמוך ביכולת מחיקת היסטוריית צ׳אט ופרטי משתמש על ידי המשתמש.	☐
4.9.9	אין לאמן את המודל על נתוני מידע רגישים של המשרד. ככל והמערכת דורשת אימון על המידע לטובת אספקת השירות, יש לקבל על כך אישור בכתב מהמשרד.	☐

4.9.10	מידע המשמש את המודל לאימון יישמר בתשתית בינה מלאכותית ייעודית (שאינה ציבורית), לא יישמר מידע/עיבוד מידע מחוץ לגבולות ישראל.	☐
4.9.11	על מקורות הנתונים המשמשים את מערכת ה-AI להיות מהימנים וחוקיים.	☐
4.9.12	על המערכת לתמוך במנגנון סינון תכנים מתקדמים לפי רשימות מילים אסורות/מותרות, הגדרות סיווג תכנים וכדומה.	☐
4.9.13	יש לקבוע ערך ברירת מחדל מתאים לפרמטר "טמפרטורה" במודלי שפה (השולט ברנדומליות התגובות), אשר יאזן בין יצירתיות וגיוון תגובות לבין צפיות, עקביות ובטיחות תגובות.	☐
4.9.14	יש להגדיר מגבלות סבירות אורך קלט (פרומפטים) והפלט (תגובות) של מערכות AI, כדי למנוע ניצול לרעה של המערכת (כגון התקפות מניעת שירות - Denial of Service) או יצירת תגובות ארוכות מדי ולא רלוונטיות.	☐

4.10 מסמכים נדרשים מטעם הספק	
4.10.1	**על הספק לצרף את כל המסמכים הבאים:**
4.10.1.1	הסמכת ISO27001 של הספק.
4.10.1.2	הסמכות, תקנים וסטנדרטים נוספים בהיבטי אבטחת מידע ופרטיות בהם מוסמך הספק כגון PCI / HIPPA / SOC2.
4.10.1.3	מיפוי מידע רגיש/חסוי הנשמר במערכת.
4.10.1.4	פירוט תהליכים ארגוניים ואמצעי אבטחה לצמצום סיכונים והתמודדות עם איומי סייבר ושרשרת אספקה.
4.10.1.5	נוהל קליטת עובד.
4.10.1.6	שרטוטי ארכיטקטורה של המערכת ומיפוי ממשקים.
4.10.1.7	פירוט המתודולוגיה ותהליכי אבטחת המידע במחזור חיי הפיתוח של המערכת.
4.10.1.8	דו"ח עדכני של מבדק חדירה (PT) של המערכת.
4.10.1.9	נהלי גיבוי, שחזור.
4.10.1.10	נוהל זיהוי ותגובה לאירועי סייבר (Incident Response).