



לשכת היועץ המשפטי

19 פברואר 2026

לכבוד
המזכיר המשותף בהליך

הנדון: הבהרה מס' 3
מפ/1639/25 מכרז לרכישת רישוי, הקמה, הטמעה ותחזוקה של מערכת בטיחות מקיפה

בהמשך לשאלות הבהרה שנתקבלו בידי קרן קימת לישראל (להלן: "המזמינה" ו/או "קק"ל")
עד ליום 25.12.2025 עד השעה 12:00, מצ"ב תשובות כדלקמן:

סידורי	החלק במסמכי המכרז שאליו מתייחסת השאלה	הסעיף במסמכי המכרז/ בחוזה/ בנספח	השאלה	התשובה
1	נספח א' 1.1 למכרז - הצעת המחיר	6.2 רישוי בסיסי: א'	האם הכוונה היא לזכות שימוש בלתי מוגבלת שאינה תלויה בתוקף ההתקשרות החוזית, או לזכות שימוש הקשורה לתקופת ההתקשרות ולתשלום דמי הרישוי והתחזוקה בפועל? וכיצד סעיף זה מתיישב עם מנגנון התמחור והעדכון השנתי המבוסס על מספר משתמשים פעילים?	זכות השימוש מותנית בקיום התקשרות חוזית בתוקף ובתשלום דמי הרישוי והתחזוקה השוטפים. עלות הרישוי תעודכן אחת לשנה בהתאם למספר המשתמשים הפעילים בפועל בהתאם לרשימה שתשלח מטעם קק"ל בטרם חידוש הרישוי, בדבר כמות המשתמשים בפועל. למען הסר ספק, מנגנון התוספת/גרירה יבוצע במדרגות של 5 משתמשים (רגילים/מנהלים) כמפורט בעמוד 47. יובהר כי זכות השימוש למזמינה היא ללא הגבלת זמן במסגרת תקופת ההתקשרות, כלומר לא יידרש תשלום נוסף מעבר לדמי הרישוי השנתיים בגין עצם זכות השימוש.
2	נספח ג' 1 - מימוש	5. שינויים ושיפורים	חובת שיתוף הפעולה והעברת המידע כאמור בסעיף זה תתבצע באמצעות תיעוד, ממשקים ונתונים, אנו מבהירים שהיא אינה כוללת העברת קוד מקור או זכויות קניין רוחני של המציע.	חובת שיתוף הפעולה כוללת תיעוד, ממשקים ונתונים. דרישה זו אינה כוללת העברת קוד מקור או אלגוריתמים של המציע
3	דרישות כלליות וחוייט	7.2.12 במסמך	המערכת תאפשר עבודה במצב לא מקוון (Offline) עם סנכרון	המערכת נדרשת לתמוך ביכולות

לשכת היועץ המשפטי

Offline עבור תהליכי שטח ודיווח. היקף התהליכים והמידע שיוגשו במצב זה, לרבות היבטי אבטחת מידע וסנכרון נתונים, יוגדרו באופן סופי בשלב האפיון המפורט של הפרויקט, וזאת בהתאם ליכולות המובנות של מוצר המדף המוצע (Out of the Box).	הדרישות הפונקציונליות אוטומטי של הנתונים ברגע שהחיבור לרשת יחודש- האם תוכלו לפרט מה הנתונים/המודולים/התהליכים החשובים ביותר? או שזה כל יכולות האפליקציה? לדוגמא האם תרצו שלכל מי שיש את האפליקציה ואת הרשאות המשתמש הנכונות יוכל לראות נתוני עובדים רגישים גם במצב ללא קליטה? כלומר שרשימת אנשים תישמר לו על הטלפון. או שיותר מדובר על ביצוע מבדקים או דיווח על מפגעים מכל מקום ללא תלות בקליטה?		משתמש	
המערכת נדרשת לאפשר ניהול ומעקב אחר הקצאת ציוד מגן אישי ברמת העובד, לרבות סוג הציוד, מועד ההפקה ותוקף או מועד נדרש לחידוש. בנוסף, עד להשלמת התממשקות עתידית למערכת ה-ERP הארגונית, המערכת תידרש לאפשר קבלת תמונת מצב ארגונית של ציוד המגן האישי לצורכי בקרה ודיווח בטיחותיים, על בסיס הנתונים המנוהלים בה. המערכת תאפשר הפקת דוחות ותצוגות ניהוליות הקשורות לכיסוי הבטיחותי של ציוד מגן אישי ברמת העובד וברמה הארגונית.	ניהול מלאי ציוד מגן אישי, האם מדובר ברישום של איזה ציוד נופק לאיזה עובד? או ממש כמות של נעלי בטיחות לצורך העניין במחסן וכל מסירה גורעת מהמלאי? נודה לפירוט נוסף.. האם צריך דוחות מיוחדים?	7.3.11 ג במסמך הדרישות הפונקציונליות	מעקב אחר הקצאת ציוד מיגון אישי (צמ"א)	4
המערכת נדרשת לקבל נתונים ממערכות הארגון, כגון המערכת הפיננסית, לצורך הצגת חיווי ובקרה על ניצול תקציב יחידת הבטיחות. עיקר הדרישה היא ריכוז המידע במקום אחד לצורכי מעקב, בקרה וקבלת תמונת מצב ניהולית.	ניהול תקציבי ורכש הקשורים ליחידת הבטיחות- נודה לפירוט מה נדרש מהמערכת לעשות? רק לקבל נתונים ופיננסים בממשק ולהציג אותם? או שצריכים לבצע חישובים פיננסים בתוך מערכת הבטיחות עצמה? אם כן, איזה חישובים?	7.3.18 במסמך הדרישות הפונקציונליות	ניהול תקציבי ורכש הקשורים ליחידת הבטיחות.	5

לשכת היועץ המשפטי

היקף הממשק, לרבות אופן צריכת הנתונים (קריאה בלבד או עדכון חוזר), וכן אפיון תתי-הסעיפים לניהול פנימי במערכת הנבחרת, יוגדרו באופן סופי בשלב האפיון המפורט של הפרויקט, בהתאם לצרכי הארגון וליכולות המובנות של מוצר המדף המוצע.				
המערכת נדרשת לתמוך בהצגת מיקומי פעילות בכלל ושל קבלנים בפרט על גבי מפה (GIS) על בסיס נצ (10 ספרות). החיווי יכול להתבצע באמצעות: - יכולות מיקום מובנות במערכת ו/או באפליקציה המוצעת על ידי הספק, לרבות שימוש ב-GPS של מכשיר הקצה. - קליטת נתוני מיקום ממערכות חיצוניות של קק"ל ו/או של הקבלן, ככל שיהיו. אופן העברת הנתונים, אפיון הממשקים, זהות מערכות המקור ורמת הפירוט יוגדרו בשלב האפיון המפורט. ככל שיעשה שימוש במערכות צד ג', האחריות על הנגשת הנתונים בפורמט הנתמך על ידי המערכת תהיה באחריות המזמינה.	המערכת תאפשר קבלת חיווי וצפייה במיקומי פעילות של קבלנים בשטח (על בסיס דיווחי קבלן או נתוני מיקום ממערכות אחרות, ככל שיהיו) - איך הנתונים האלו מגיעים? בלייב מהשטח? חיישנים? או דיווח של הקבלן ישירות במערכת/אפליקציה? נודה לפירוט נוסף	7.3.8 ה' / ו' במסמך הדרישות הפונקציונליות	בקרת בטיחות קבלנים בשטח	6
המערכת נדרשת לכלול מודול לניהול 'מרכז ידע' או 'ספריית נהלים',	ממשק תקנים וספרים מול המוסד לבטיחות גהות ולנגישות- נודה לפירוט נוסף מה הציפייה מהמערכת	7.6.1 במסמך הדרישות הפונקציונליות	ממשק מערכות חיצוניות עם	7



קרן קימת לישראל
K K L - J N F

לשכת היועץ המשפטי

המאפשר ליחידת הבטיחות להעלות, לנהל ולהנגיש למשתמשים מסמכים, תקנים וקישורים חיצוניים (כגון לאתר המוסד לבטיחות וגיהות). באחריות המציע לספק את התשתית הטכנולוגית והיכולת להזנת התכנים. המערכת תתמוך עקרונית ביכולת התממשקות למקורות מידע חיצוניים (API) ככל שיהיו זמינים ונגישים טכנולוגית, כאשר אפיון הממשק והמשמעויות הנגזרות ממנו יבוצעו בשלב האפיון המפורט.				
כל זכות יצירה מקורית וזכות יוצרים הנובעת מאספקת השירותים תהיה בבעלותה הבלעדית של המזמינה. הספק מצהיר שבחתימתו על הסכם ההתקשרות הוא מוותר על כל טענה או תביעה לעניין בעלות או זכות קניין א זכות רוחנית כלשהי על תוצרי השירות. מבלי לגרוע מתוקף האמור לעיל, מסמכים ותוצרים, לרבות שיטות עבודה, ידע מקצועי, Know How, מתודולוגיות ורעיונות אשר הינן רכוש הספק או גורם אחר כלשהו קודם למועד התחלת אספקת השירותים יישארו בבעלות הספק או אותו גורם. בכפוף לתשלום מלוא התמורה המגיעה לספק, הספק יעניק לקק"ל זכות שימוש בלתי חוזרת, לא ייחודית, ללא תשלום תמורה כלשהי, בכל	בהיעדר הוראה מפורשת במסמכי המכרז וההסכם המצורף בדבר העברת זכויות קניין רוחני, הצעת המציע נערכה על בסיס ההנחה כי למזמינה מוקנית זכות שימוש במערכת ובפיתוחים הייעודיים שיפותחו במסגרת הפרויקט אך ורק למשך תקופת ההתקשרות, וכי זכויות הקניין הרוחני בפיתוחים כאמור אינן נגרעות מזכויות הספק, והספק אינו מוגבל מלעשות שימוש בפיתוחים אלה, כולם או חלקם, במסגרת מוצריו ו/או התקשרויותיו עם צדדים שלישיים.	כללי	כללי	8

לשכת היועץ המשפטי

זכות יוצרים, זכות מסחרית וזכות קניינית אחרת, בנוגע לשירותים. קק"ל תהיה רשאית לעשות בתוצרי השירות שינויים ותוספות, להעבירם לאחר או לעשות בהם כל שימוש שתראה לנכון.				
הממשקים הארגוניים ייחשפו באמצעות מפרט OpenAPI (Swagger). במקרה של עדכון ממשק, תתבצע הקפצת גרסה בהתאם לכללי SemVer תוך שמירה על תאימות לאחור ככל הניתן. ככלל, רוב הממשקים המפורטים בסעיף 7.3 הנם ממשקי קריאה (Pull/Push). ככל שגדרת כתיבה חזרה למערכות המקור הדבר יבוצע בהתאם ליכולות ה-API- שיעמדו לרשות הספק. אפיון השדות המדויק והגדרת הלוגיקה לכתיבה יבוצע בשלב האפיון המפורט.	במפרט מצוין כי נדרש ממשק דו-כיווני מול מספר מערכות. נבקש להבהיר עבור כל מערכת מהי רמת הכתיבה הנדרשת: האם יש צפי לשינוי בסכמות של המערכות אשר יתממשקו למערכת הבטיחות, באיזו תדירות ומהו המנגנון המתוכנן לעדכון על השינויים?	7.2	מסמכי המכרז	9
ככלל, רוב הממשקים המפורטים בסעיף 7.3 מיועדים לצורכי קבלת מידע, חיווי ובקרה (Pull/Push), לרבות קבלת סטטוסים, אישורי הצלחה או כישלון (ACK) ולוגים. עם זאת, במקרים נקודתיים ייתכן ותידרש גם כתיבת נתונים בפועל למערכות המקור (כגון עדכון סטטוס או יצירה/עדכון רשומות), וזאת בהתאם לצרכים העסקיים וליכולות ה-API של המערכות המתממשקות.	האם נדרשת כתיבת נתונים בפועל (לדוגמה: עדכון סטטוס הכשרה ב-LMS, יצירת מפגע ב-GIS, או עדכון פרוטוקולים ב-apiCommittees)? או שמא מדובר בממשק לצורכי חיווי ובקרה בלבד (קבלת אישורי הצלחה/כישלון - ACK, ולוגים)?	7.3.13 7.3.8 במסמך הדרישות הפונקציונליות	דרישות פונקציונליות_מכרז מערכת בטיחות.xlsx	10



קרן קימת לישראל
K K L - J N F

לשכת היועץ המשפטי

ההחלטה אילו תהליכים יכללו כתיבה, אפיון השדות, הלוגיקה העסקית ואופן המימוש יוגדרו באופן סופי בשלב האפיון המפורט של הפרויקט.				
מסמכי API עדכניים (כגון OpenAPI/Swagger) ודוגמאות Payload יימסרו לספק הזוכה בלבד, כחלק מתהליך האפיון והיישום, ובכפוף להרשאות ולמדיניות אבטחת המידע של קק"ל.	לצורך הערכת מורכבות הפיתוח, נבקש לקבל מסמכי API עדכניים (כגון Swagger/OpenAPI) ודוגמאות Payload עבור כלל המערכות המוזכרות (HR, LMS, GIS, ERP, Projects, וכו').	7.3 במסמך הדרישות הפונקציונליות	דרישות פונקציונליות_מכרז מערכת בטיחות.xlsx"	11
מערכת ה HR הארגונית של קק"ל מהווה את 'מקור האמת' הבלעדי לנתוני העובדים והמבנה הארגוני. המערכת תבצע סנכרון שוטף של נתוני היסוד הנדרשים (כגון שם, מזהה עובד, שיוך יחידתי) לצורך ניהול רציף של תהליכי בטיחות, הדרכות ומשימות בתוך המערכת. עדכון נתונים (עובד חדש, עזיבת עובד או שינוי תפקיד) יבוצע במערכת ה HR בלבד ויסונכרן למערכת הבטיחות באופן אוטומטי. מנגנון ההזדהות (Authentication) יבוצע מול שירותי ה AD הארגוניים בסטנדרט SSO כמפורט בנספח אבטחת מידע • תדירות הסנכרון, מנגנון העדכון (יומי, מבוסס אירועים ו/או לפי דרישה) וכן המיפוי בין תפקידי העובדים	על מנת להבטיח סנכרון נכון של המבנה הארגוני, נבקש לדעת: מהו מקור האמת לנתוני העובדים (מערכת ה-HR, ה-Active Directory, או שילוב ביניהן)? מהי תדירות העדכון הנדרשת וכיצד מוגדר המיפוי בין תפקיד העובד בארגון להרשאותיו במערכת הבטיחות?	7.3.10 ד במסמך הדרישות הפונקציונליות	דרישות פונקציונליות_מכרז מערכת בטיחות.xlsx"	12

לשכת היועץ המשפטי

להרשאות במערכת הבטיחות, יוגדרו ויאושרו בשלב האפיון המפורט, בהתאם לדרישות הלקוח, למדיניות אבטחת המידע ולמבנה הארגוני בפועל. הסנכרון יבוצע באמצעות ממשקי API מבוקרים, בהתאם לארכיטקטורה הארגונית של קק"ל.				
אופן העבודה של כל ממשק (Online/Push, Batch/Pull), רמות השירות, זמני תגובה, מדיניות Retry ונפחי נתונים צפויים יוגדרו בשלב האפיון המפורט עם הספק הזוכה. אופן עבודת הממשקים ושיטת הסנכרון יותאמו לצרכים התפעוליים של כל תהליך ויוגדרו סופית בשלב האפיון המפורט, וזאת בין היתר בהתאם ליכולות הטכנולוגיות של ה-API- וההרשאות שיועמדו לרשות הספק. בהתאם למפורט בנספחי המכרז (נספח ג' (סעיף 11 ונספח ג'1 סעיף 6). מובהר כי הנתונים בנספחים אלו מהווים בסיס להערכה, והגדרות סופיות ומפורטות יסוכמו בין הצדדים בשלב האפיון בהתאם לארכיטקטורת הפתרון שתוצע.	נבקש להגדיר עבור כל ממשק את אופן העבודה הנדרש: שיטת העבודה: האם נדרש סנכרון בזמן אמת (Online/Push) או סנכרון תקופתי (Batch/Pull)? רמת שירות: מהם זמני התגובה הנדרשים, מדיניות ניסיונות חוזרים (Retry) במקרה של כשל, ומהם נפחי הנתונים הצפויים?	7.3 במסמך הדרישות הפונקציונליות	דרישות פונקציונליות_מכרז מערכת בטיחות.xlsx	13
מערכות פעילות כיום עבור מערכות פעילות במועד ההתקשרות, הממשקים יבוצעו כחלק משלבי ההקמה הראשוניים של הפרויקט, בהתאם	חלק מהמערכות המוזכרות (כמו ERP או LMS) עשויות להיות בשלבי הקמה. נבקש להבהיר: אילו מהמערכות פעילות כיום ואילו מוגדרות כ"עתידיות"? עבור מערכות עתידיות - האם	7.3 א 7.3.11 א 7.3.13 א 7.3.16 במסמך הדרישות הפונקציונליות	דרישות פונקציונליות_מכרז מערכת בטיחות.xlsx	14

לשכת היועץ המשפטי

לאפיון שיאושך. מערכות עתידיות עבור מערכות שטרם הוקמו או טרם עלו לאוויר (כגון LMS או ניהול מצאי), המציע נדרש להבטיח מוכנות טכנולוגית מראש, לרבות: • הגדרת מבנה נתונים ושדות רלוונטיים. • מוכנות לממשקי API סטנדרטיים. מוכנות זו תאפשר חיבור עתידי למערכות אלה ללא צורך בפרויקט הסבה מהותי או פיתוח נוסף משמעותי. עד להקמת המערכות העתידיות, העבודה תתבצע באמצעות הקמה ידנית במערכת הבטיחות ו-או באמצעות טעינת קבצים (Excel/CSV), בהתאם לצרכי הארגון.	הציפייה היא לעבודה ידנית בשלב הראשון, או שנדרשת הכנה טכנית (מבנה נתונים ושדות) שתאפשר חיבור מהיר בעתיד ללא צורך בהסבה?			
--	---	--	--	--

לתשומת לב המשתתפים, בעקבות שאלות ההבהרה שנשאלו, יחולו השינויים הבאים במסמכי המכרז:

1. עמ' 41 הסעיף 6.2 ב' יימחק
2. עמ' 41 סעיף 6.3 א' ישתנה כדלקמן: התמורה בגין רישוי השימוש במערכת תשולם אחת לשנה עם חידוש הרישוי, בהתאם לרשימת משתמשים פעילים שתועבר ע"י המזמינה.
3. עמ' 41 הסעיף 6.3 ב' יימחק
4. עמ' 41 סעיף 6.3 ג' ישתנה כדלקמן: עלות הרישוי תעודכן אחת לשנה בהתאם לרשימה שתועבר כמפורט בסעיף א' לעיל
5. עמ' 61 סעיף 4.1 ישתנה כדלקמן: תוקף של הסכם זה הינו החל מיום חתימתו, אולם תקופת הרישוי בפועל תהא לתקופה של שלוש (3) שנים שתחל ממועד סיום ההקמה וה"עלייה לאוויר" (להלן: "תקופת ההתקשרות הראשונה").
6. עמ' 100 נספח ג(3) "סודיות, פרטיות ואבטחת מידע לרכישת מערכות תוכנה כשירות" יוחלף בנוסח המעודכן המצורף להבהרה זו **כנספח פרטיות ואבטחת מידע**

מועד אחרון להגשת הצעות נדחה עד ליום ה' 9.3.2026 עד השעה 12:00.



לשכת היועץ המשפטי

*** הבהרה זו נועדה להוסיף על מסמכי המכרז/ההליך ואין בה כדי לגרוע מהם בכל צורה שהיא.

*** יש לצרף מסמך זה להצעה שתוגש כשהוא חתום על ידי המציע.

חתימה + חותמת המציע _____

בכבוד רב,

איה כהן לומר

איה כהן לומר, עו"ד

לשכת היועץ המשפטי

נספח פרטיות ואבטחת מידע - לחתימת הספק הזוכה במכרז

מצד	בין: קרן קיימת לישראל (להלן: "המזמינה")
מצד	אחד; _____ [שם], ח.פ. כתובת מלאה פרטי קשר (מספר טלפון; דוא"ל; פקס) (להלן: "הספק") שני; והואיל וההספק זכה במכרז שפורסם על ידי המזמינה לאחר שעמד בכל תנאי הסף להתמודדות במכרז לרבות עמידה בהוראות נספח פרטיות ואבטחת מידע לרכישת מערכות תוכנה כשירות; והואיל וההצדדים התקשרו ביניהם בהסכם מיום _____, על פיו הספק יספק למזמינה שירותי _____ ("השירותים" ו"ההסכם", "ההתקשרות", בהתאמה); והואיל וכחלק מההתקשרות, הספק עשוי לעבד מידע (כגדירתו להלן), ובכלל זה לבצע פעולות שונות במאגרי המידע של המזמינה ובמערכות המאגר, לרבות עיבוד המידע, גישה ישירה למידע ו/או יחזיק במידע; והואיל וברצון הצדדים להגדיר תחומי האחריות של כל אחד מהצדדים להסכם ולהסדיר את נושא הגנת הפרטיות, אבטחת המידע וכל הנדרש לצורך הסדרת השימוש במידע על פי דין; והואיל וההצדדים מעוניינים לצרף נספח זה להסכם, על מנת שיהיה חלק בלתי נפרד ממנו.

לפיכך, הוסכם, הוצהר והותנה בין הצדדים כדלקמן:

1. **הגדרות:**
 - 1.1 **חוקי הגנת הפרטיות** – חוק הגנת הפרטיות, התשמ"א-1981, התקנות שהותקנו ו/או יותקנו מכוחו, לרבות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("תקנות הגנת הפרטיות"), וק הנחיות הרשות להגנת הפרטיות.
 - 1.2 **מידע אישי** – "מידע אישי" ו"מידע בעל רגישות מיוחדת" כהגדרתם בחוק הגנת הפרטיות, התשמ"א-1981.
 - 1.3 **מידע** – כל מידע או נתון, לרבות כל מידע אישי, הנוגע למזמינה ו/או למי מטעמה, לרבות עובדיה ו/או לקוחותיה, שהועבר ו/או יועבר לספק או שניתנה לספק גישה אליו על ידי המזמינה ו/או מי מטעמה, לרבות מידע אישי ממאגרי המידע של המזמינה ומידע כאמור שהספק יעבד כחלק ממתן השירותים למזמינה וכן מידע שנאסף, נצבר, נוצר או התקבל אצל הספק במסגרת שירותיו למזמינה.
 - 1.4 **מערכות המאגר** – מערכות המשמשות את המידע של המזמינה ואשר יש להן חשיבות בהיבטי אבטחת מידע.
 - 1.5 **נושא מידע** – אדם שהמידע האישי נאסף אודותיו.
 - 1.6 **תקנות אבטחת המידע** – תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017.
 - 1.7 המונחים "עיבוד", "מאגר מידע", "מחזיק", "בעל שליטה", תהא פרשנותם בהתאם להוראות חוקי הגנת הפרטיות.
2. **הצהרות והתחייבויות הספק בנוגע למידע:**
 - 2.1 הספק מצהיר כי ידוע לו שבמסגרת הזמנת העבודה הספק עשוי להיחשף למידע.
 - 2.2 הספק מצהיר ומבין שלצורך נספח זה, המזמינה היא בעל השליטה במאגר המידע לעניין מידע, והספק הוא מחזיק מאגר מידע. הספק מאשר שיחולו עליו כל החובות החלות על מחזיק במאגר מידע בהתאם לחוקי הגנת הפרטיות וכי הוא ימלא אחר כל החובות האמורות לגבי מאגרי המידע של המזמינה מהם יעבד מידע במסגרת מתן השירותים. במידה והמזמינה תהא מחזיק במאגר מידע לצורך ההסכם בין הצדדים, הספק יהיה מחזיק משנה מטעם המזמינה.

לשכת היועץ המשפטי

- 2.3 הספק מתחייב לפעול על פי כל דין, לרבות הוראות חוקי הגנת הפרטיות, ובפרט בנוגע לעיבוד המידע.
 - 2.4 הספק מצהיר ומתחייב בזאת, כי הוא בעל ניסיון קודם בעיבוד מידע, ויש לו את היכולת, ידע ורקע בתחום ביצוע השירותים, כפי שהוגדרו בהסכם ("מטרת השירות"). וכי לא קיים כל חשש לניגוד עניינים מובנה או סיכון אחר לשימוש פסול במידע על ידי מי מטעמו. הספק יודא כי פעולות עיבוד המידע (באם יידרש במסגרת השירות המבוקש) ייעשו בהתאם להוראות תוספת א' לנספח זה. הספק יעדכן את המזמינה במידה ומטרת השירות דורשת את עדכון תוספת א'.
 - 2.5 הספק מצהיר ומתחייב בזאת כי לא ישתמש במידע בניגוד למטרה לשמה נמסר או באופן שמהווה פגיעה בפרטיות.
 - 2.6 הספק לא יעבד או ישתמש במידע, אלא לשם ביצוע מטרת השירות וכי כל המידע שברשותו יועבר לבעלי התפקידים הנדרשים בלבד לצורך מטרת השירות ("בעלי התפקידים המורשים").
 - 2.7 הספק ימנה ממונה על הגנת הפרטיות, אלא אם לא נדרש לכך בהתאם להוראות חוקי הגנת הפרטיות. פרטי הממונה ימסרו למזמינה לבקשתה.
 - 2.8 במידה והספק יידרש לאסוף ו/או לייצר ו/או לצבור מידע, הספק מצהיר כי הפעולות הללו ייעשו אך ורק בדרכים חוקיות וכי לא יעשה שימוש במאגרי מידע בלתי חוקיים.
 - 2.9 הספק יגדיר נוהל אבטחת מידע וימנה ממונה אבטחת מידע, ככל הנדרש לעשות זאת לפי חוקי הגנת הפרטיות.
3. כוח אדם; הדרכות וסודיות:
- 3.1 הספק מתחייב כי יבצע הדרכות עתיות לכל בעלי התפקידים המורשים בדבר מטרת השירות, הוראות חוק הגנת הפרטיות ותקנותיו, פיתוח מאובטח ובפרט תקנות אבטחת המידע. על פי דרישת המזמינה, יציג הספק העתק בדבר רשימת ההדרכות אשר בוצעו לבעלי התפקידים המורשים בהתאם למסמך זה.
 - 3.2 הספק מתחייב כי לא הוא ו/או מי מטעמו יגלו מידע שהגיע אליו ו/או למי מטעמו בתוקף תפקידו כעובד, כמנהל, כמחזיק של מאגר מידע או כנותן שירות אחר הכרוך בעיבוד המידע, אלא לצורך מטרת השירות וכי ידועות לו הוראות סעיף 16 לחוק הגנת הפרטיות ותקנה 19 לתקנות אבטחת המידע.
 - 3.3 הספק מתחייב כי לספק ו/או לעובדיו ו/או לקבלני משנה מאושרים, תהא הרשאת גישה למידע של המזמינה, אך ורק לשם מטרת השירות ולא מעבר לכך, על פי הגדרתם תפקידים. הספק יערוך רשימת בעלי תפקידים מורשים ויעבירה למזמינה, בכפוף לדרישתה.
 - 3.4 הספק יודא כי כלל בעלי התפקידים המורשים מטעמו חתומים על הסכמי סודיות אשר יבטיחו את שמירת סודיות המידע.
4. אבטחת מידע:
- 4.1 הספק מתחייב ליישם בנוגע למידע, במהלך תקופת ההתקשרות וכל עוד הספק מעבד מידע, מנגנוני אבטחת מידע העומדים בסטנדרטים הגבוהים ביותר המקובלים בשוק בעת הרלוונטית ואשר לא פוחדים מדרישות הוראות חוקי הגנת הפרטיות ובכל מקרה במנגנוני אבטחת מידע העומדים בכל דרישות המזמינה לעניין אבטחת מידע המפורטות בהסכם ובנספח זה, וכפי שיהיו מעת לעת.
 - 4.2 ככל שמדובר בספק המספק שירותי תוכנה, הספק מתחייב ליישם בכל עת בנוגע למידע מנגנוני אבטחת מידע העומדים בדרישות המזמינה כאמור בתוספת ב' (מנגנוני אבטחת מידע), בתוספת ג' (עקרונות לפיתוח ותחזוקה מאובטחים) ובתוספת ד' (יישום ארכיטקטורה מאובטחת בעק – Security Standards) לנספח זה. למען הסר ספק, תוספות ב', ג' ו-ד' יחולו אך ורק מקום בו הספק מספק שירותי תוכנה כאמור, ואינן חלות על ספק שאינו מספק שירותי תוכנה. המזמינה רשאית לעדכן תוספות אלו לפי הצורך. הספק יעדכן מעת לעת ובהתאם לצורך את מנגנוני אבטחת המידע באופן שיעמדו בדרישות חוקי הגנת הפרטיות ובאופן שלא יפחת מדרישות האמורות בתוספות להסכם.
 - 4.3 על הספק, לפי דרישה של המזמינה, להגיש למזמינה תוכנית עבודה מלאה ומפורטת ותיק מערכת הכולל מפרט טכנולוגי מלא של כלל חלקי המערכת, שכבות הגנה, ארכיטקטורה, טכנולוגיות, תוכנות וממשקים, טרם הטמעת המערכת אצל המזמינה.
5. מיקור-חוצ:
- 5.1 הספק לא יעביר ו/או יעבד את המידע, אלא כאמור בנספח זה.

לשכת היועץ המשפטי

- 5.2 במקרה בו יידרש הספק להעביר את המידע לצדדים שלישיים לצורך ביצוע מטרת השירות ("קבלן משנה"), הספק יקבל את אישור המזמינה לכך, מראש ובכתב. במידה והמזמינה הביעה התנגדות מנומקת וסבירה לכך שהספק לא יעביר את המידע לקבלן המשנה, הספק יעשה את מירב המאמצים לספק את השירותים מבלי להעביר את המידע לקבלן המשנה. הצדדים ינהלו מרשם ובו פרטי כל קבלן משנה שאושר על ידי המזמינה ("קבלן משנה מאושר").
- 5.3 הספק יודיע למזמינה, זמן סביר מראש, ובכתב, על כוונתו להחליף או לצרף קבלן משנה.
- 5.4 לגבי כל קבלן משנה מאושר, הספק יודא כי:
- 5.5 כל סיכוני אבטחת המידע הכרוכים בהתקשרות נבחנו וקיבלו מענה הולם על ידי קבלן המשנה;
- 5.6 נחתם הסכם המסדיר את חובות קבלן המשנה מול הספק והמזמינה, בהתאם לדרישות תקנה 15 לתקנות אבטחת המידע;
- 5.7 במידה וההתקשרות עם קבלן המשנה כרוכה בהעברת מידע אל מחוץ לגבולות מדינת ישראל, העברת המידע עומדת בכל דרישות החוק, לרבות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001.
- 5.8 מבלי לגרוע מהוראות ההסכם, הספק יישא באחריות מלאה לכל מעשה או מחדל של קבלני המשנה המאושרים, והפרה כלשהי של הוראות נספח זה תיחשב להפרה של הספק, על כל המשתמע מכך.
6. **זכויות נושאי מידע:**
- 6.1 הספק יעמוד בחובותיו הנוגעות למימוש זכויות נושאי מידע ויסייע למזמינה במימוש חובותיה מול נושאי המידע. הספק ייעדכן את המזמינה באופן מדי, ולא יאוחר מ-24 שעות מקבלת פניה מנושא מידע הקשורה למידע ולא ישיב לפניה מבלי לקבל את אישור המזמינה לכך.
- 6.2 הספק יעדכן את המזמינה באופן מדי ובכתב, לגבי כל פניה, בעל-פה או בכתב, מטעם רשות מנהלית, ובפרט הרשות להגנת הפרטיות, וכן פניה מגורמי חקירה או אכיפה, הנוגעת לשירותים ו/או למידע.
7. **שימוש בכלי בינה מלאכותית:**
- 7.1 הספק מתחייב כי לא יעשה כל שימוש בכלי בינה מלאכותית לצורך עיבוד המידע, אלא באישור המזמינה מראש ובכתב. מבלי לגרוע מהאמור לעיל, ככל שיעבד מידע באמצעות כלי בינה מלאכותית, הספק מתחייב כי:
- 7.2 יפעל בהתאם להוראות המזמינה המנויות בתוספת ה' לנספח זה (הוראות שימוש בכלי בינה מלאכותית).
- 7.3 לא יעשה שימוש כאמור במידע באופן המפר את הוראות ההסכם (לרבות, אך לא רק, חובות סודיות ואבטחת מידע) או את הוראות הדין החל והנחיות רגולטוריות מחייבות הנוגעות לכלי בינה מלאכותית.
- 7.4 לא יכלול את המידע במערך נתוני האימון (training data; validation data) של כלים או מודלים של מערכת בינה מלאכותית, אלא אם כן התקבלה הסכמת המזמינה בכתב. לעניין סעיף זה, "מערכת בינה מלאכותית" היא מערכת ממוכנת אשר מסיקה מהקלט המוזן לה כיצד להפיק תחזיות, תוכן, המלצות או החלטות שיכולות להשפיע על הפרט או על פעילותה של המזמינה או על פעילותו של הספק (לרבות כלי בינה מלאכותית יוצרת [generative] שבו נוצר תוכן חדש באמצעות אלגוריתמים בתגובה לפקודות קלט (prompt)), או כמשמעות מונח זה בדין החל והנחיות רגולטוריות מחייבות.
8. **אירוע אבטחת מידע:**
- 8.1 הספק ידווח למנהל אבטחת המידע של המזמינה (באמצעות הטלפון 050-7245008) ולמוקד SOC המספק למזמינה שירותי ניטור אבטחת מידע (באמצעות הטלפון 077-4030846) באופן מדי לאחר גילוי אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה ("אירוע אבטחת מידע"). הדיווח יכלול את כל המידע הקיים, נכון למועד הדיווח, על נסיבות אירוע אבטחת המידע והפעולות שננקטו ועתידות להינקט על ידי הספק לצורך הטיפול באירוע והשלכותיו.
- 8.2 הספק אחראי על הטיפול באירוע אבטחת המידע וכן יישא בעלויות הטיפול באירוע אבטחת המידע, חקירת האירוע ויישום תובנות לאחר סיום הטיפול באירוע. במידת הצורך, המזמינה תעביר הנחיות ודגשים מטעמה ביחס לאופן שבו היא מצפה שאירוע אבטחת המידע יטופל. הספק ימלא אחר הוראות המזמינה, ככל שינתנו, ביחס לחובות

לשכת היועץ המשפטי

- הנוגעות לאירוע אבטחת המידע, בהתאם לחוקי הגנת הפרטיות, לרבות דיווח לרשות ועדכון נושאי המידע (ככל שאלו נדרשים).
- 8.3 הספק לא יענה לפניות מצדדים שלישיים הנוגעות לאירוע אבטחת המידע וכן לא ישתף מיוזמתו פרטים על אודות אירוע האבטחה, מבלי לקבל את אישור המזמינה לכך מראש ובכתב, אלא אם הוראות הדין מחייבות את הספק להימנע מעדכון כאמור.
9. **מחיקה או השבת מידע:**
- 9.1 הספק מצהיר ומתחייב בזאת כי עם סיום ההתקשרות, מכל סיבה שהיא, יעביר למזמינה עותק תקין ושלם של גיבוי המידע האחרון. לאחר מכן על פי דרישתה הראשונה של המזמינה, כל המידע שהגיע לרשות הספק במסגרת השירותים יימחק באופן מלא ותוך זמן סביר ולא יאוחר מ-30 ימים לאחר תום ההתקשרות בין הצדדים או פניית המזמינה. לבקשת המזמינה, יציג הספק למזמין תצהיר חתום על ידי מורשי החתימה של הספק המאמת ביצוע פעולות מחיקה כאמור.
- 9.2 במידה והספק מחויב בהתאם להוראות הדין לשמור העתק מן המידע, יעשה הספק את מירב המאמצים לשמור את המידע בצורה אנונימית. במידה ולא ניתן למחוק את הפרטים המזהים מהמידע, יעדכן הספק, מראש ובכתב, את המזמינה כי הוא נדרש על פי דין לשמור העתק מהמידע.
- 9.3 ככל שקיימת הוראה בדין המחייבת שמירת המידע אצל הספק, הספק מצהיר ומתחייב בזאת כי אמצעי האבטחה שהוגדרו בהתקשרות עם המזמינה, יישארו בתוקף לכל אורך תקופת שמירת המידע.
10. **ביקורות; דיווח שנתי:**
- 10.1 מוסכם כי נציגיה המוסמכים של המזמינה, בתיאום סביר מראש עם הספק, יהיו רשאים לבצע ביקורות על אופן התנהלותו של הספק בסוגיות של השימוש במידע ואבטחתו. מבלי לגרוע מהאמור לעיל, הספק יעמיד לעיון המזמינה, תוך זמן סביר, מסמכים המעידים על עמידתו בחובות אבטחת המידע החלות עליו ובפרט לגבי עמידתו בתקנות אבטחת המידע וישיב על שאלוני ביקורת מטעם המזמינה.
- 10.2 הספק מתחייב להגיש למזמינה, בתום 12 חודשים מיום חתימת נספח זה, ולאחר מכן ובמשך כל תקופת ההתקשרות וכן כל עוד הספק מעבד מידע, דיווח על אופן ביצוע חובותיו בהתאם לנספח זה והוראות חוקי הגנת הפרטיות. הספק יעביר למזמינה את הדיווח ופרטים נוספים הדרושים למזמינה על מנת להדגים את עמידת בחוקי הגנת הפרטיות לשביעות רצונה של המזמינה. ככל ויתגלה כי הספק אינו עומד בחוקי הגנת הפרטיות ובהנחיות הסכם זה, הספק יפעל בהקדם לתקן את האמור, על חשבונו.
11. **שיפוי:**
- 11.1 הספק מתחייב לשפות את המזמינה ו/או כל מי מטעמה, באופן מדי, בגין כל תשלום, פיצויים, עיצום כספי, שכר טרחת עורכי דין ומומחים וכל הוצאה אחרת ששולמה על-ידי המזמינה או מי מטעמה בעקבות כל הליך מטעם רשות מוסמכת נגד המזמינה או מי מטעמה, בקשר עם כל טענה כלשהי של כל צד שלישי בנוגע לחובות הספק מכוח נספח זה ומכוח חוקי הגנת הפרטיות, ואשר האחריות לגביהם חלה בהתאם להוראות ההסכם, נספח זה או בהתאם לחוקי הגנת הפרטיות, על הספק.
12. **כללי:**
- 12.1 מבלי לגרוע מאחריות הספק על פי מסמך זה ו/או על פי כל דין, מתחייב הספק לערוך ולקיים על חשבונו, לטובתו ולטובת המזמינה, למשך כל תקופת ההתקשרות, כל ביטוח הנדרש ממנו על פי דין וכן בהתאם לדרישות המקדמיות להתקשרות עם המזמינה.
- 12.2 התחייבויות הספק המפורטות בנספח זה ימשיכו לחול כל עוד הספק יעבד מידע, גם לאחר סיומו של ההסכם ונספח זה, מכל סיבה שהיא, למעט אם המידע נשמר בצורה אנונימית, לאחר שמאפייניהם של נושאי המידע הוסרו באופן סופי ובלתי ניתן לשינוי.
- 12.3 הספק מצהיר כי הינו מודע לכל סמכויותיו של ראש הרשות להגנת הפרטיות וכי הוא עומד וימשיך לעמוד במהלך כל תקופת ההתקשרות בין הצדדים בחובותיו כלפי ראש הרשות להגנת הפרטיות, לרבות סמכויות הפיקוח של ראש הרשות להגנת הפרטיות אצל הספק בהקשר של פעילות מיקור החוץ שלו עבור המזמינה.
- 12.4 הספק יעמיד איש קשר מטעמו אשר יעמוד בקשר עם נציג מטעם המזמינה. אנשי הקשר יתאמו ביניהם את כל הטעון ברור בקשר להדרכה והטמעה של השירות, תוך הסבר מפורש על אודות השימוש המותר במידע.



קרן קימת לישראל
K K L - J N F

לשכת היועץ המשפטי

12.5 הספק מצהיר בזאת כי אין במסמך זה כדי לגרוע מחובותיו וזכויותיו על פי חוקי הגנת הפרטיות, ההסכם ודינים אחרים החלים על השירותים הניתנים על ידי הספק.

חתימה

שם הספק

תאריך

לשכת היועץ המשפטי

תוספת א' – פעולות עיבוד מידע

תוספת זו מפרטת את פעולות עיבוד המידע המותרות, בהתאם להוראות תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 :

1. המידע שהספק רשאי לעבד ומטרות השימוש בו לצורכי ההתקשרות :
עיבוד המידע יעשה למטרת השירות, כהגדרתה בנספח זה, בהתאם להוראות ההסכם וכפי שיסכימו הצדדים מעת לעת.
2. סוג העיבוד שהספק רשאי לעשות :
הספק רשאי לבצע אך ורק את פעולות עיבוד מידע הדרושות למטרת השירות, כהגדרתה בנספח זה, בהתאם להוראות ההסכם וכפי שיסכימו הצדדים מעת לעת.
3. מערכות המאגר שהספק רשאי לגשת אליהן :
הספק רשאי לגשת אך ורק למערכות מידע של המזמינה, אשר פורטו בהסכם ו/או שאושרו על ידי מראש ובכתב.

לשכת היועץ המשפטי

תוספת ב' – הוראות אבטחת מידע

1. הספק ישמור את המידע של המזמינה וכן את התשתיות והמערכות המשמשות את המידע, במקום מוגן, המונע חדירה וכניסה אליו ללא הרשאה והתואם את אופי פעילות מאגר המידע ורגישות המידע. הספק יבצע בקרה ותיעוד של הכניסה והיציאה מאתרים בהם מצויות מערכות המידע וכן בקרה ותיעוד של הכנסה והוצאת ציוד אל מערכות בהן מעובד המידע.
2. הספק יגביל/ימנע אפשרות חיבור התקנים ניידים וינקוט באמצעי ההגנה הנדרשים. במידה והספק מאפשר שימוש בהתקנים ניידים, הספק יקבע נוהל מסודר לשימוש בהתקנים כאמור.
3. הספק לא יחבר את המערכות שבהן מעובד מידע לרשת האינטרנט או לרשת ציבורית אחרת, ללא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש.
4. בגישה מרחוק באמצעות רשת האינטרנט או רשת ציבורית אחרת, הספק יעשה שימוש גם באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה.
5. הספק יהיה מותעד לתקן ISO 27001: 2022, כאשר פעילות פיתוח הרלוונטית כלולה בתחום ההתעדה, אלא אם צוין אחרת על ידי המזמינה.
6. הספק יעביר לגורמי אבטחת המידע של המזמינה, על פי בקשתם ובהתאם לצורך, תרשים רשת מעודכן של סביבת מאגרי המידע של המזמינה ומערכות המאגר. התרשים יכלול את תחנות הקצה, רכיבי הרשת, רכיבי אבטחת המידע ומערכות האחסון המשמשות לצורך מתן השירותים. התרשים יתאר את היצרנים ואת מערכות ההפעלה שבשימוש.
7. הספק יידרש ליישם מנגנוני הגנה והקשחה עבור בסיסי הנתונים שבשימוש המערכת, בהתאם לנהוג ולמיטב הפרקטיקות בתעשייה, ובהתאמה לרמת הרגישות ולסוגי המידע הנשמרים בהם. ההגנות יכללו, בין היתר, בקורות גישה, הצפנת מידע, ניהול הרשאות וניטור פעילויות, ביצוע מבדקי חדירה וסקר סיכונים. היקף ההגנות והאמצעים שיושמו ייגזרו מאופי המידע וייעשו בתיאום עם המזמינה.
8. הספק יודא הפרדה, ככל הניתן, בין המערכות אשר ניתן לגשת מהן למידע שבמאגר, לבין מערכות מחשוב אחרות שמשמשות את הספק.
9. תיושם ותתועד בקרה (LOG) להרשאות הגישה וכניסות משתמשים ומנהלים לכלל המערכות בהן קיים מידע השייך למזמינה. פרטי הלוג יכללו, לכל הפחות, את כתובת IP של הגולש, זהות המשתמש (במערכות בהן מיושמים תהליכי הזדהות) והרשמה עבור הגולשים/מנהלי המערכת (כגון אזור אישי, מערכת ניהול וכד'); התאריך והשעה של ניסיון הגישה; רכיב המערכת שאליו בוצע ניסיון הגישה; סוג הגישה, היקפה ואם ניסיון הגישה הצליח או נדחה. נתוני התיעוד ישמרו לפרק זמן המוגדר בחוקתקנות, ובכל מקרה לא פחות מ-24 חודשים. כמו כן, המערכת תתמוך בהעברת לוג אירועים למערך Siem/Soc של המזמינה, במידת הצורך.
10. הספק יספק למזמינה ויטמיע במערכתיו עדכוני גרסה, תיקוני תכנה, עדכוני אבטחה, עדכוני טבלאות מערכת באופן אוטומטי וללא תוספת תשלום. כמו כן ידווח לגורמי המזמינה על כל

לשכת היועץ המשפטי

- שינוי או עדכון. התקנת עדכוני גרסאות או כל שינוי במערכת הדורש השבתת השרות או שעלול לשבש את השרות, יתואם עם המזמינה מבעוד מועד.
11. גיבוי בסיס הנתונים יתבצע בצורה שתאפשר שחזור גרנולרי לפי דרישה. תדירות הגיבוי תאפשר, לכל הפחות, שחזור ברזולוציה של 4 שעות למשך חודש ימים, ברזולוציה חודשית למשך שנה, וברזולוציה שנתית למשך שבע שנים. ביצוע שחזור רבעוני יזום, ידווח למזמינה בכתב. שחזור מלא כולל דיווח יהא אחת לשנה.
12. במערכות בהן מיושמים תהליכי הזדהות/הרשמה עבור הגולשים/מנהלי המערכת (כגון אזור אישי, מערכת ניהול וכד') הספק יחיל לגבי מערכות המאפשרות גישה למאגרי המידע ולמידע, מדיניות סיסמאות בהתאם לדרישות תקנות אבטחת המידע (מספר תווים מינימלי, סיסמה מורכבת, תדירות החלפה, טיפול בתקלות אימות וכדומה).
13. הספק יודא כי העברת מידע תעשה תוך שימוש באמצעי אבטחת תקשורת ומידע מקובלים, לרבות באמצעות שימוש בשיטות הצפנה מקובלות.
14. באחריות הספק לבצע מבדקי חדירה למערכות שמסופקות למזמינה במסגרת השירותים בטרם תחילת מתן השירותים. דוחות המבדקים יוצגו למזמינה לפי דרישה, לרבות אישור מצד בודק חיצוני כי, כלל הממצאים תוקנו. המזמינה שומרת לעצמה את הזכות לביצוע בדיקות חדירות תקופתיות (PENETRATION TESTS) נוספות למערכת. אם ימצאו פערים בין התחייבויות הספק לפי נספח זה ולבין תוצאות בדיקות החדירות, הספק יפעל ללא דיחוי וללא עלות לתיקונם של פערים אלו ופערים הנוגעים לאי עמידה בדרישות הדין. במידה והמזמינה תבקש לעדכן את הדרישותיה בנוגע להגנת המידע, היא תמסור על כך הודעה בכתב לספק, אשר יבחן את משמעויות עמידתו בדרישות המעודכנות, למעט אם העדכון נובע מדרישות רגולטוריות החלות על הספק ו/או שיחולו על הספק בקשר עם ביצוע השירותים. במידה ומימוש של הדרישות הנ"ל יהיה כרוך בעלויות נוספות, אלו יבוצעו בכפוף לתמורה נוספת, אשר תפורט בהצעה שתשלח על-ידי הספק בנושא. ככל והדרישות נובעות מדרישות רגולטוריות החלות על הספק על-פי דין בנושא הגנת מידע ופרטיות בקשר עם השירותים, אלו יבוצעו על חשבון הספק ללא תמורה נוספת. ככל והדרישות נובעות מדרישות רגולטוריות שאינן חלות על הספק (למשל, דרישות אשר חלות על המזמינה) ידונו הצדדים בתום לב לגבי התמורה לספק.

לשכת היועץ המשפטי

תוספת ג' – עקרונות לפיתוח ותחזוקה מאובטחים

1. המערכת תרוץ בהרשאות משתמש הנמוכות ביותר שאפשר ברמת שרתים ובסיסי נתונים.
2. במערכות בהן מיושמים תהליכי הזדהות/הרשמה עבור הגולשים\מנהלי המערכת (כגון אזור אישי, מערכת ניהול וכד'), תוגדר מדיניות סיסמאות חזקה בגישה למערכת למשתמשים ומנהלים. יש לתמוך ללא סייג בשימוש ב-OTP/MFA בכל כניסה.
3. במערכות בהן מיושמים תהליכי הזדהות/הרשמה עבור הגולשים\מנהלי המערכת (כגון אזור אישי, מערכת ניהול וכד') תתקיים הגבלה של מספר התחברויות מקבילות עבור כל משתמש, ממקומות שונים בו זמנית וכן הגדרת ניתוק SESSION לאחר פרק זמן של חוסר פעילות שלא יעלה על פרק הזמן שיוגדר ע"י המזמינה.
4. במערכות בהן מיושמים תהליכי הזדהות/הרשמה עבור הגולשים\מנהלי המערכת (כגון אזור אישי, מערכת ניהול וכד') תיושם נעילת משתמש לאחר מספר ניסיונות כושלים ושחרור ע"י מנהל המערכת. בנוסף לשחרור המשתמש ע"י המנהל, יש להוסיף פונקציית מבחן טיורינג [CAPTCHA] בניהול גורם רשמי ונפוץ (למשל גוגל) למניעת גישת מכונה למערכת.
5. יישום הגבלות על התחברות מרחוק לצורך ניהול האפליקציה ייעשה ב-VPN בלבד או הגבלת גישה לממשקי ניהול לכתובות IP מסוימות בלבד.
6. במערכות בהן מיושמים תהליכי הזדהות/הרשמה עבור הגולשים\מנהלי המערכת (כגון איזור אישי, מערכת ניהול וכד') ובמקרים בהם יאושר ע"י המזמינה להתבסס על מקורות הזדהות המקומיים במערכת, ייושם מנגנון אחסון סיסמאות מוצפן (שאינו Clear Text) באתר HASHED PASSWORDS בפרוטוקול 256 SHA לפחות או מקבילו.
7. קיום מערכת FW, IPS ואנטי וירוס להגנה על שרתי האפליקציה.
8. שימוש בתעודות SSL מאושרות ומעודכנות להצפנת מידע רגיש העובר בתווך ציבורי מול משתמשים וממשקי API בפרוטוקול TLS 1.2 לפחות.
9. שימוש במנגנונים להגנה בפני התקפות מניעת שירות (DDOS) והתקפות אפליקטיביות OWASP TOP 10 על האתר, WAF או הוסטינג או רכישה לרבות הפעלת הגנת GEO וחסימת גישה בהתאם למדיניות המזמינה.
10. ביצוע וולידציה של קלטים של משתמשים לפי הגדרה מראש בצד השרת.
11. שימוש במנגנונים למניעת מתקפות כמו SQL INJECTION, XSS, FILE INCLUSION, buffer over flow וכדומה.
12. תתקיים הפרדה בין שרתי בסיס נתונים לשרתי המערכת ומערכת הניהול.
13. העברת מידע בתווך מוצפן בלבד בכלל סוגי הממשקים.
14. במערכות בהן מיושמים תהליכי הזדהות/הרשמה עבור הגולשים\מנהלי המערכת (כגון איזור אישי, מערכת ניהול וכד'), יתבצע יישום וניהול מנגנון הרשאות המאפשר ניהול הרשאות במערכת על בסיס עקרונות הצורך לדעת והפרדת תפקידים בהתאם לאפיון, כאשר כל רמת הרשאה תיוצג ע"י קבוצת מורשים במקור ההזדהות (IDP) של המזמינה.
15. במערכות בהן מיושמים תהליכי הזדהות/הרשמה עבור הגולשים\מנהלי המערכת (כגון איזור אישי, מערכת ניהול וכד'), יישמרו לוגים של גישות משתמשים למערכת וביצוע פעולות רגישות באפליקציה כמו ייצוא נתונים, כולל שליחת התראות על היקפי ייצוא חריגים.

לשכת היועץ המשפטי

16. הספק יפעל לשדרוג גרסאות תוכנה ובפרט במקרה של פרסום על חולשות קריטיות בגרסאות הקיימות של רכיבי התוכנה השונים.
17. הספק ינהל רשימה של סוגי הקוד הפתוח והרישיונות שחלים על כל קוד פתוח בו נעשה שימוש במסגרת מתן השירותים למזמינה. לא יעשה שימוש בספריות קוד פתוח שאינן נתמכות ומתעדכנות. הספק יבחן, בטרם שימוש בקוד פתוח במערכות ושירותים עבור המזמינה, את כל סיכוני האבטחה הידועים הקשורים לשימוש בקוד פתוח זה, לרבות בחינת חולשות ידועות, ויפעל לצמצום סיכוני אבטחת המידע שבשימוש בקוד כאמור.

תוספת ד' – יישום ארכיטקטורה מאובטחת בענן – Security Standards

1. הספק יוודא שימוש ב-API או STORED PROCEDURES על מנת למנוע ממשק ישיר בין המשתמש לשרת בסיס הנתונים.
2. הספק יבצע הפרדה בין בסיס הנתונים של המזמינה לבין בסיסי נתונים של לקוחות אחרים.
3. הספק יישם שימוש בפרוטוקול Https בכל דפי היישום אם המערכת בענן או על גבי האינטרנט. באם מדובר במערכת עם ממשק WEB, תתקיים מניעת אפשרות למניפולציה של כתובת ה-URL (חוסר יכולת לשנות UID בסוף הדף וכן מניעת יכולת לשנות או להוסיף דפי משנה).
4. הספק יגדיר רשימת ערכים וטווחים מותרים לכלל שדות קלט, תוך עדיפות לרשימה סגורה של ערכים ויקבל את אישור המזמינה לרשימה זו.
5. אין לחשוף למשתמש הקצה הודעות שגיאה אפליקטיביות העלולות להסגיר את סוג התשתית, גרסה, קוד וטבלאות בתוך היישום. יש לשקף הודעה גנרית בלבד.
6. העלאת קבצים למערכת :
תתקיים הגבלת סוגי הקבצים שניתן להעלות לאפליקציה לפורמטים מורשים בלבד על בסיס זיהוי חד ערכי של סוג הקובץ.
א. במקרים בהם מתבצעת העלאת קבצים למערכת ושמירתם בשרתי הספק - יש לוודא כי קובץ המועלה לשרת יעבור תהליך סניטציה ויישמר בשרת כקובץ בעל סיומת NON EXECUTABLE).
ב. במקרים בהם מתבצעת העלאת קבצים למערכת ונתון העברתם לתשתיות המזמינה באמצעות קריאות API, קק"ל תחשוף עבור ספק המערכת API ייעודי לצורך ביצוע תהליכי סניטציה
7. הספק יוודא כי אין בדו"חות המופקים מהמערכת חשיפה של שדות שלא נדרשים.
8. גרסת מערכת הפעלה, דפדפנים, בסיסי נתונים ותשתיות תוכנה בגרסאות מתקדמות (עד גרסה אחת אחורה בלבד (N-1)).
9. העברת אפליקציה מסביבת פיתוח לייצור תתבצע בצורה מבוקרת.
10. לא יעשה שימוש בנתונים אמיתיים בסביבת הפיתוח.
11. במידה וקיימים ממשקים מהענן אל המערכות הארגוניות יש לתאר בפני המזמינה את הממשקים בצורה מפורטת.

לשכת היועץ המשפטי

12. במערכות בהן מיושמים תהליכי הזדהות\הרשמה עבור המשתמשים\מנהלי המערכת (כגון איזור אישי, מערכת ניהול וכד') נדרשת תמיכה בתצורת הזדהות SSO מול AWS\AD\ENTRAID. יש לתאר את אופן המימוש של מנגנון הזדהות (SAML, OPENID).