

## נספח הגנת הפרטיות ואבטחת מידע

נספח זה הינו בהמשך להסכם שנחתם מול חברת אדית פתרונות תוכנה בע"מ ("הספק"), ומהווה חלק בלתי נפרד ממנו.

### 1. הגדרות:

כל המונחים שלא הוגדרו בנספח זה, תהא פרשנותם בהתאם להוראות ההסכם.

- 1.1. "הדין החל" – פירושו חוק הגנת הפרטיות תשמ"א-1981 (להלן - "חוק הפרטיות") והתקנות שהותקנו על פיו (ובפרט תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, (להלן - "התקנות"), הנחיות רשם מאגרי המידע, ובפרט הנחיה מס' 2/2011 בדבר שימוש מיקור חוץ לעיבוד מידע אישי, וכן כל הנחיה או הוראה חקיקתית ו/או מנהלית שתחול או שיחולו על הספק בקשר עם מתן השירותים לפי ההסכם.
- 1.2. "מידע אישי" – נתונים, מידע או מערך מידע שניתן לזהות באמצעותו, במישרין או בעקיפין, אדם פרטי.
- 1.3. "מידע אישי של החברה" – כל מידע אישי שהועבר ו/או יועבר לספק או שניתנה לספק גישה אליו על ידי החברה ו/או מי מטעמה, לרבות מידע אישי ממאגרי המידע של החברה ומידע אישי שהספק יעבד כחלק ממתן השירותים לחברה.
- 1.4. "נושא מידע" – אדם שהמידע האישי נאסף אודותיו.
- 1.5. "עיבוד" – כל פעולה המבוצעת על מידע אישי או באמצעות מידע אישי, לרבות שינוי, גישה, אחסון, שמירה, העברה, גישה, תיקון והעתקה של מידע אישי.
- 1.6. "פגיעה באבטחת מידע" – פירושה שימוש או גישה בלתי מורשית למידע אישי או שיבוש של מידע אישי במאגר;
- 1.7. "מאגר מידע" או "המאגר" – אוסף נתוני מידע אישי של החברה, המוחזק באמצעי פיזי, מגנטי או אופטי.
- 1.8. "שירותים" – פירושה השירותים שהספק מעניק לחברה בהתאם להסכם ולנספח זה.
- 1.9. "החברה" – הלקוח אשר התקשר בהסכם התקשרות עם חברת אדית פתרונות תוכנה בע"מ, הינו בגדר בעל השליטה במאגר המידע, כהגדרתו ובהתאם להוראות חוק הגנת הפרטיות.
- 1.10. "הספק" – להלן חברת אדית פתרונות תוכנה בע"מ.
- 1.11. "מחזיק המאגר" – גורם חיצוני לבעל השליטה במאגר המידע, המעבד מידע עבורו. לעניין זה, חברת אדית פתרונות תוכנה בע"מ מהווה מחזיקת מאגר המידע, ואינה מהווה בעלת השליטה במאגר המידע או מנהלת המאגר.
- 1.12. "בעל השליטה" – מי שקובע, לבדו או יחד עם אחר, את מטרות עיבוד המידע שבמאגר המידע או גוף שהוא או בעל תפקיד בו הוסמך בחיקוק לעבד מידע במאגר המידע. החברה אשר לה הסכם התקשרות עם אדית פתרונות תוכנה בע"מ, הינה בעלת השליטה במאגר המידע.
- 1.13. "מנהל המאגר" – בעל שליטה במאגר מידע, ולעניין גוף ציבורי כהגדרתו בסעיף 23 לחוק, המנהל הכללי של גוף שבעלותו או בהחזקתו מאגר מידע או מי שהמנהל הכללי הסמיכו לנהל את המאגר. לעניין זה, החברה שלה הסכם התקשרות עם אדית פתרונות תוכנה בע"מ, מהווה הגורם המנהל את מאגר המידע.

### 2. הצהרות והתחייבויות הספק

- 2.1. הספק מצהיר כי במסגרת מתן השירותים לחברה הספק עשוי להיחשף למידע אישי של החברה.
- 2.2. הספק מצהיר ומתחייב כי בעת מתן השירותים לחברה הוא יעמוד בכל עת בכל הוראות הדין החל. בכלל זה, מצהיר הספק ומאשר כי הוא מתמצא בדין החל וכי הוא יבצע את כל החובות והדרישות שנקבעו על ידי רשות הגנת הפרטיות (לשעבר רמו"ט).
- 2.3. החברה (להלן: לקוח אדית פתרונות תוכנה בע"מ) הינה הבעלים הבלעדיים של מאגרי המידע ואין באמור בנספח ו/או בהסכם כדי להעניק לספק (להלן: אדית פתרונות תוכנה בע"מ) זכויות קנייניות במידע האישי. החברה רשאית, אך לא מחויבת, להנחות את הספק בקשר לאופן עיבוד המידע האישי והספק מתחייב לעשות כל שביכולתו על מנת למלא אחר התחייבויות החברה, כפי שיינתנו מעת לעת. יובהר כי הספק (להלן: אדית פתרונות תוכנה בע"מ) הינה מהווה כמחזיקת המאגר בלבד, ואינה בעלת המאגר או בעלת השליטה במאגרי המידע.
- 2.4. הספק מצהיר ומתחייב להקצות את המשאבים הדרושים לו לשם מילוי הוראות הדין החל וכן הוראות נספח זה.
- 2.5. הספק מצהיר ומתחייב בזאת, כי הוא בעל ניסיון קודם בעיבוד מידע, ויש לו את היכולת, ידע ורקע בתחום ביצוע השירותים, כפי שהוגדרו בהסכם.

### 3. חובות הספק במסגרת עיבוד מידע אישי

- 3.1. הספק יעבד את המידע האישי עבור החברה אך ורק למטרת הענקת השירותים לפי ההסכם, ורק בדרך שנקבעה לכך בהסכם ובנספח, ולא לכל מטרה אחרת, אלא אם קיבל הוראה מפורשת בכתב מאת החברה לעשות זאת.
- 3.2. הספק יבצע גישה רק למערכות אשר הכרחיות לצורך מתן השירות ובכפוף למנגנוני האבטחה הנדרשים ע"י החברה.
- 3.3. הספק מתחייב לנהל הרשאות גישה למידע אישי, ובכלל זה יקנה למשתמשיו הרשאות מינימליות (Least Privileged) על בסיס הצורך לדעת (Need to Know) לצורך מילוי תפקידים וינקוט באמצעים למניעת גישה של גורמים בלתי מורשים למידע אישי. בנוסף, על הספק לנהל רישום עדכני של כל מורשי הגישה למאגר ולמנוע גישה מכל אדם שאין צורך שייחשף למידע של החברה.
- 3.4. הספק לא יעניק גישה למידע האישי לעובדיו, יועציו או מי מטעמו בטרם החתים אותם על כתב התחייבות לשמירה על סודיות, אבטחת המידע ופרטיות נושאי המידע שפרטיהם כלולים במאגר. הספק יהיה אחראי כלפי החברה בגין כל מעשה ו/או מחדל של מי מעובדיו, יועציו ו/או מטעמו בקשר עם הפרת הוראות נספח זה.
- 3.5. הספק יעניק לבעלי תפקידים הרשאות גישה למאגר המידע בכפוף לקיום הדרכות תקופתיות בנושא חובות הגנת הפרטיות ואבטחת מידע שחלות על הספק מתוקף הדין החל ו/או נספח זה.
- 3.6. הספק יטמיע אמצעי אבטחה וניטור שבאמצעותם הספק יתעד כל גישה למערכות המאגר כהגדרתם להלן.
- 3.7. הספק יפתח, יטמיע ויאכפוף מדיניות אבטחת מידע אשר תכלול לפחות את הנושאים הבאים ("מדיניות אבטחת מידע"):
  - 3.7.1. מיפוי של כלל אמצעי האבטחה שנוקט הספק ביחס למערכות המאגר;
  - 3.7.2. הוראות באשר לאופן ניהול הרשאות הגישה למאגר ואמצעי בקרת הגישה למידע האישי והפעולות הנעשות בו;
  - 3.7.3. הנחיות למורשי הגישה למידע אישי ולמערכות המאגר;
  - 3.7.4. סקירת הסיכונים שחשוף להם המידע האישי במסגרת פעילותו השוטפת של הספק;
  - 3.7.5. הוראות באשר לאופן התייעוד, הניטור והזיהוי של איומים על מערכות המאגר ועל אירועים בהם יש חשש לפגיעה באבטחת המידע;
  - 3.7.6. הוראות בדבר עריכת ביקורות תקופתיות כאמור בסעיף 7 להלן;
  - 3.7.7. הוראות לעניין אופן ההתמודדות של הספק עם אירועי אבטחת מידע (כהגדרתם להלן).
- 3.8. הספק יערוך מיפוי של הסביבה התפעולית של מאגר המידע, בכלל זה יכין הספק רשימת מצאי הכוללת את כלל מערכות המידע, תוכנות, ממשקים, תשתיות רכיבי חומרה ורכיבי תקשורת שהספק מפעיל בסביבת המאגר לשם תפעולו השוטף של המאגר ("מערכות המאגר"). הספק יעדכן את רשימת המצאי המפורטת בסעיף זה מעת לעת, אך בכל מקרה בעת ביצוע שינויים מהותיים בסביבה התפעולית, במערכות המאגר או בתהליכי עיבוד המידע.
- 3.9. הספק, עובדיו, קבלניו, וסוכניו לא יאספו ולא יבקשו לקבל מידע אישי באופן ישיר מנושאי המידע, למעט במקרה ונושא המידע הסכים לכך או כאשר החברה התירה מפורשות וכתב את האיסוף או את הבקשה לקבל מידע האישי.
- 3.10. הספק, עובדיו, קבלניו וסוכניו לא יעבדו כל מידע אישי עבור החברה בדרך שאינה מתיישבת עם הדין החל או לכל מטרה אחרת שלא הותרה באופן מפורש או משתמע בהסכם ו/או בנספח זה.

### 4. אבטחת מידע

- 4.1. הספק מתחייב ליישם בנוגע למידע האישי של החברה, במהלך תקופת ההתקשרות וכל עוד הספק מעבד מידע אישי של החברה, מנגנוני אבטחת מידע העומדים בהוראות הדין החל ובסטנדרטים הגבוהים ביותר המקובלים בשוק בעת הרלוונטית. ובכל מקרה במנגנוני אבטחת מידע העומדים בכל דרישות החברה לעניין אבטחת מידע המפורטות בהסכם ובנספח זה, וכפי שיהיו מעת לעת.
- 4.2. הספק יקיים הפרדה לוגית בין מערכות המאגר לבין מערכות מחשוב המשמשות את הספק לכל צורך שאינו קשור במישרין למתן השירותים לחברה. בכל חיבור של מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, יתקין הספק אמצעי הגנה מתאימים מפני פגיעה באבטחת המידע.
- 4.3. הספק ישמור את המידע האישי של החברה אך ורק כל עוד יש צורך בכך על מנת להגשים את המטרות שלשמן הועבר לספק, או כפי שיידרש על פי הדין החל.
- 4.4. הספק יעדכן באופן שוטף את מערכות המאגר, לרבות את התוכנות המותקנות במערכות המאגר, בעדכוני אבטחת מידע. בהפעלת מערכות המאגר, הספק לא יעשה שימוש ברכיבי תוכנה ו/או חומרה שהיצרן לא תומך בהיבטי האבטחה שלהן.

- 4.5. הספק יפעל להתקנה והפעלה של תוכנות אבטחה מקצועיות ומעודכנות כנגד תוכנות זדוניות, פעולות זדוניות וחזירות ברשת ומחשבי הספק שמהם מבוצעת הכניסה מרחוק לרשת של הארגון או מאוחסן בהם מידע של הארגון.
- 4.6. הספק יפעל להחתמת עובדיו או מי מטעמו הניגשים לרשת של הארגון ו/או מערכות הארגון או מקבלים גישה אחרת למידע של הארגון על הצהרות התחייבות לשמירה מוחלטת על סודיות המידע של הארגון וקיום נהלי אבטחת מידע של הארגון.
- 4.7. הספק יפעל לקיום כל דרישות חוק הגנת הפרטיות, תקנותיו והנחיות מכוח החוק בקשר לשירותים המסופקים על ידו לארגון ואשר חלות על הארגון והספק.
- 4.8. המידע של הארגון יאוחסן בגבולות מדינת ישראל או באיחוד אירופאי ואמריקה בלבד. אסור להעביר מידע ללא אישור הארגון בכתב למקומות אחרים.
- 4.9. השימוש בהרשאות הגישה למערכות המידע של הארגון שהוענקו לספק ומי מטעמו יעשה אך ורק לצורך מילוי המטלות שהוטלו על הספק במסגרת הסכם ההתקשרות עם הספק.
- 4.10. לא יבוצעו פעולות החורגות את תחום הפעילות שהותר לספק כגון: ניסיונות כניסה לחשבון משתמש אחר, ניסיונות כניסה לתיקיות לא מורשות וכדומה.
- 4.11. הספק ינקוט בכל האמצעים הסבירים לא לאפשר לגורם לא מורשה, לעשות שימוש בהרשאות הגישה שניתנו לו.
- 4.12. הספק יפעל לפי הנחיות אבטחת מידע של הארגון כפי שיעוברו מעת לעת על ידי הגורמים מוסמכים מטעמה ויפעל לתקן בהקדם כל ליקויי אבטחה שיתגלו על ידי הארגון וגורמים מטעמה על חשבונו.
- 4.13. הספק יעביר או יקבל את המידע הכולל נתונים אישיים באמצעות תווך או מדיה מוצפנים ומאובטחים בלבד.
- 4.14. תקני אבטחה: הספק מוסמך לתקני **ISO 27001, ISO 27799** בהסמכת מכוון התקנים מאז שנת 2020.
- 4.15. הספק יבצע **מבדקי חזירה וסקרי סיכונים תקופתיים (ולכל הפחות אחת ל-18 חודשים)** ברמה התשתיתית והאפליקטיבית לאיתור חולשות אבטחה. הספק יתחייב לטיפול מהיר בממצאים ברמה גבוהה קריטית.
- 4.16. **ככל שזה רלוונטי לתחום פעילותו** יישם הספק כללי פיתוח מאובטח ויישום ארכיטקטורה מאובטחת בענן. (ראו סעיף 12 -נספחים)
- 4.17. התחייבות זו מחייבת את הספק או מי מטעמו במשך פעילותו מול רשת המחשבים, מערכות המידע וגישה למידע של הארגון ולאחר סיום עבודתו מול הארגון.

## 5. העברת מידע אישי

- 5.1. הספק לא יעביר ו/או יעבד את המידע האישי של החברה, אלא כאמור בנספח זה.
- 5.2. במקרה בו יידרש הספק להעביר את המידע לצדדים שלישיים לצורך ביצוע השירותים, יקבל הספק את אישור החברה לכך, מראש ובכתב. במידה והחברה 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.
- 5.3. היה ותאשר החברה בכתב לספק לגלות מידע אישי לקבלן משנה של הספק ("קבלן משנה"), הרי שלפני כל גילוי כאמור, יתקשר הספק בהסכם כתוב, תקף ואכיף עם קבלן המשנה שמכיל לכל הפחות תנאים דומים במהותם לתנאים המופיעים בנספח זה.
- 5.4. במידה וההתקשרות עם קבלן המשנה תהא כרוכה בהעברת מידע אל מחוץ לגבולות מדינת ישראל, העברת המידע תעמוד בכל דרישות הדין החל, לרבות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001.
- 5.5. הספק יעשה שימוש במנגנוני הצפנה מקובלים עבור כל העברה של מידע אישי לצד שלישי ועבור כל התחברות מרחוק למערכות המאגר.
- 5.6. מבלי לגרוע מהוראות ההסכם, הספק יהיה אחראי לפעילות קבלני המשנה מטעמו בקשר למתן השירותים, בהתאם להוראות הסכם זה.

## 6. זכויות נושאי מידע

- 6.1. הספק יספק את המידע והסיוע שיידרש על ידי החברה כך שהחברה תוכל למלא אחר דרישות הדין החל בנושא עיון, תיקון ומחיקה של מידע אישי לפי בקשה של נושאי המידע. מבלי לגרוע מן האמור, כאשר נושא המידע ו/או נציגו המורשה יגיש בקשה בכתב לספק לצורך מימוש זכויותיו כאמור, הספק יודיע לחברה על קבלת הבקשה בהקדם האפשרי, ולא יאוחר משני (2) ימי עסקים מקבלת הבקשה, בצירוף הפרטים הרלוונטיים, ולא ישיב לפניו מבלי לקבל את אישור החברה לכך.
- 6.2. היה ובעקבות הבקשה כאמור בסעיף 6.1 לעיל יתברר כי המידע האישי אינו מדויק, אינו שלם, אינו ברור או אינו עדכני, יכולה החברה לערוך את התיקונים או השינויים המתאימים באופן עצמאי באמצעות המערכת המקוונת לאספקת השירותים.

## 7. ביקורת, תיעוד וניטור

- 7.1. הספק מתחייב לתעד את הפעילות הנעשית במערכות המאגר, לרבות (אך לא רק) תיעוד ניסיונות הגישה למערכות המאגר, מחיקה ו/או שינוי של מידע אישי ושינוי של הרשאות הגישה למערכות המאגר ("מנגנון התייעוד"). מנגנון התייעוד יאסוף לפחות את הנתונים הבאים: זהות המשתמש, התאריך והשעה של הפעולה, מקור ביצוע הפעולה (כתובת אינטרנט או שם מחשב), רכיב המערכת בו בוצעה הפעולה, סוג הפעולה, האם הפעולה הצליחה או נכשלה.
- 7.2. נתוני התייעוד שיפיק מנגנון התייעוד יישמרו לאורך תקופת ההסכם בין הצדדים, אלא אם החברה הורתה אחרת בכתב.
- 7.3. אם הנושא לא דובר, יעמוד הספק בדרישות תקנה 10 לתקנות הגנת הפרטיות המחייבות שמירת לוגים ממערכות המאגר וכן ממערכות האבטחה למשך שנתיים לכל הפחות. הלוגים יישמרו במערכות מקומית באופן המאפשר שליפה ותחקור מהיר.
- 7.4. הספק ימסור לחברה, לבקשתה, אישור בכתב לפיו קיים את חובותיו בהתאם לנספח זה והוראות הדין החל.
- 7.5. הספק מתחייב לדווח, פעם בשנה לכל הפחות, על עמידותו של הספק בהוראות אלו והוראות הדין החל.
- 7.6. הספק מאפשר ללקוחות המוגדרים כלקוחות גדולים, ולנציגי אלה בתחום אבטחת המידע, לבצע בתיאום מראש, סקרים וביקורות לצורך בחינת עמידתו של הספק בהתחייבויותיו לפי נספח זה. הספק רשאי להטיל מגבלות נוספות על ביצוע סקרים וביקורות כדי להגן על סודותיו המסחריים או על אמצעי האבטחה שלו. עריכת סקרים וביקורות כאמור מותנית בחתימת הלקוח או שלוחיו על **התחייבות לשמירת סודיות**, בנוסח המקובל אצל הספק במועד הרלוונטי. הספק רשאי, לפי שיקול דעתו הסביר, לסרב לביצוע סקרים וביקורות על ידי לקוחות שאינם מוגדרים כלקוחות גדולים, או לדרוש התאמות נוספות לתהליך לצורך שמירה על סודיות והגנת מידע.

## 8. אירוע אבטחת מידע

- 8.1. הספק ידווח לחברה באופן מיידי ולא יאוחר מ-24 שעות מרגע גילוי מקרה שיש בו כדי להעלות חשש לפגיעה במידע האישי של החברה, לשימוש בו בלא הרשאה או לחריגה מהרשאה ("אירוע אבטחת מידע").
- 8.2. הדיווח יכלול את כל המידע הקיים, נכון למועד הדיווח, על נסיבות אירוע אבטחת המידע והפעולות שנקטו ועתידות להינקט על ידי הספק לצורך הטיפול באירוע והשלכותיו.
- 8.3. הספק יסייע לחברה למלא אחר חובותיה הנוגעות לאירוע אבטחת המידע, וכן יישא בעלויות הטיפול באירוע אבטחת המידע, חקירת האירוע ועדכון נושאי המידע, ככל שהדבר נדרש מכוח הדין החל.
- 8.4. הספק לא יענה לפניית מצדדים שלישיים הנוגעות לאירוע אבטחת המידע וכן לא ישתף מיוזמתו פרטים על אודות אירוע האבטחה, מבלי לקבל את אישור החברה לכך מראש ובכתב, אלא אם הוראות הדין החל מחייבות את הספק להימנע מעדכון כאמור.

## 9. מחיקה או השבת מידע אישי

- 9.1. בהתאם להסכם ומבלי לגרוע מכלליותו, הספק ישיב, ימחק או יבער את כל המידע האישי שעליו חל נספח זה, לרבות אך ללא הגבלה, כל העותקים המקוריים וההעתקים של אותו מידע אישי, בכל מדיום שהוא, לרבות אך ללא הגבלה, כוננים קשיחים, אמצעי גיבוי, וכל מדיה מגנטית או אופטית אחרת וכל החומרים שנבעו מהמידע האישי או הכוללים אותו בתוך שלושים (30) ימים מבקשת החברה בכתב להשבה, מחיקה או ביעור מכל סיבה שהיא.
- 9.2. עם סיום המחיקה וההעברה הספק יציג לחברה אישור המאמת ביצוע פעולות המחיקה או הביעור כאמור.
- 9.3. במידה והספק מחויב בהתאם להוראות הדין לשמור העתק מן המידע האישי של החברה, יעשה הספק את מירב המאמצים לשמור את המידע בצורה אנונימית. במידה ולא ניתן למחוק את הפרטים המזהים מהמידע, יעדכן הספק, מראש ובכתב את החברה, כי הוא נדרש על פי דין לשמור העתק מהמידע האישי של החברה ויכלול בהודעה זו את הדין המחייב והמועדים הנקובים בו.
- 9.4. ככל שקיימת הוראה בדין המחייבת שמירת המידע אצל הספק, הספק מצהיר ומתחייב בזאת כי אמצעי האבטחה שהוגדרו בהתקשרות עם החברה, יישארו בתוקף לכל אורך תקופת שמירת המידע ועם הגיע מועד פג התוקף האמור בדין, יפעל לפי האמור בסעיף 9.1 לעיל.

## 10. סיום ההתקשרות

כל הסעיפים בנספח זה המחויבים מכוח הדין החל ימשיכו לחול גם לאחר פקיעתו או סיומו של ההסכם בין הצדדים, ובלבד שהספק ממשיך להחזיק במידע אישי שמקורו בחברה.

## 11. הדין החל וסדר קדימות

ככל שאין בהם סתירה לאמור בזה, הסעיפים הרלוונטיים של ההסכם (לרבות אך ללא הגבלה, לעניין סיום, אכיפה, הדין החל ופרשנות) יחולו על נספח זה. במקרה של סתירה בין הוראות נספח זה לבין הוראות ההסכם, הרי שתנאי נספח זה יגברו ויחולו.

## 12. נספחים:

### 12.1 נספח מסמך עקרונות לפיתוח ותחזוקה מאובטחים:

- האפליקציה תרוץ בהרשאות משתמש הנמוכות ביותר שאפשר ברמת שרתים ובסיסי נתונים.
- ללקוחות ניתנת האפשרות לקבוע את מדיניות הסיסמאות של הארגון שלהם בתוכנה, כולל שליטה מלאה בהחלטות כגון הפעלת הגנת FA2 או שימוש בפיצ'רים נוספים בתחום אבטחת המידע, לפי שיקול דעתם.
- הספק מספק בתוכנה אפשרות להגבלת מספר ההתחברויות של משתמש ממקומות שונים בו זמנית, וכן אפשרות לניתוק SESSION אוטומטי במקרה של חוסר פעילות למשך עד 30 דקות. אפשרויות אלו קיימות במערכת וניתנות להפעלה לפי **החלטת המשתמש**.
- הספק מספק בתוכנה אפשרות לנעילת חשבון לאחר מספר ניסיונות כניסה כושלים, עם שחרור החשבון על ידי מנהל או באמצעות CAPTCHA אפשרות זו קיימת במערכת וניתנת להפעלה, כאשר מספר הניסיונות המקסימלי וקביעת מדיניות השחרור ניתן להתאמה על ידי המשתמש, תוך שמירה על עקרונות אבטחת מידע מומלצים.
- קיימת בתוכנה אפשרות ליישום הגבלות על התחברות מרחוק לצורך ניהול האפליקציה והשימוש בה. הפעלת אפשרות זו מתבצעת במסגרת הגדרת ההרשאות של משתמשי הלקוח, וניהול התוכנה בצד הלקוח נשאר בשליטת הלקוח.
- יישום מנגנון אחסון סיסמאות מוצפן (שאינו Clear Text) באתר HASHED PASSWORDS בפרוטוקול SHA 256 לפחות או מקבילו.
- הטמעת מערכת FW, IPS ואנטי וירוס להגנה על שרתי האפליקציה
- שימוש בתעודות SSL מאושרות ומעודכנות להצפנת מידע רגיש העובר בתווך ציבורי מול משתמשים וממשקי API בפרוטוקול TLS 1.2 לפחות.
- הגנה בפני התקפות מניעת שירות (DDOS) והתקפות אפליקטיביות OWASP TOP 10 על האתר, WAF או הוסטינג או רכישה לרבות הפעלת הגנת GEO
- ביצוע וולידציה של קלטים של משתמשים לפי הגדרה מראש בצד השרת.
- שימוש במנגנונים למניעת מתקפות כמו SQL INJECTION, XSS, FILE INCLUSION, buffer over flow וכדומה.
- תתקיים הפרדה בין שרתי בסיס נתונים לשרתי ה-WEB.
- העברת מידע בתווך מוצפן בלבד בממשקים השונים.
- יישום וניהול מנגנון הרשאות משוכלל המאפשר ניהול הרשאות באפליקציה על בסיס עקרונות הצורך לדעת והפרדת תפקידים.
- יישמרו לוגים לגישות משתמשים לאפליקציה וביצוע פעולות רגישות באפליקציה כמו ייצוא נתונים.
- הספק יפעל לשדרוג גרסאות תוכנה בתדירות תקופתית של לפחות פעם בשנה ובמקרה של פרסום על חולשות קריטיות בגרסאות הקיימות של רכיבי התוכנה השונים.

12.2 נספח יישום ארכיטקטורה מאובטחת בענן – Security standarts:

1. הספק יוודא שימוש ב WEB SERVICE או PROCEDURES STORED על מנת למנוע ממשק ישיר בין המשתמש לשרת בסיס הנתונים.
2. הספק מבצע הפרדה ברורה ובטוחה בין בסיס הנתונים של הארגון לבין בסיסי הנתונים של לקוחות אחרים, באופן המבטיח כי לכל לקוח יש גישה אך ורק לנתוניו שלו.
3. הספק יישם שימוש בפרוטוקול Hhttps בכל דפי היישום אם המערכת בענן או על גבי האינטרנט. באם מדובר במערכת עם ממשק WEB, מניעת אפשרות למניפולציה של כתובת ה URL- (חוסר יכולת לשנות UID בסוף הדף, לא ניתן לשנות או להוסיף דפי משנה).
4. הספק יגדיר רשימת ערכים וטווחים מותרים לשדות קלט, תוך עדיפות לרשימה סגורה של ערכים.
5. אין לחשוף למשתמש הקצה הודעות שגיאה אפליקטיביות העלולות להסגיר קוד וטבלאות בתוך היישום. שגיאות כאלה יש לכתוב לקובץ לוג בלבד או לתת הודעה גנרית.
6. שימוש במערכות הפעלה, דפדפנים, בסיסי נתונים ותשתיות תוכנה בגרסאות נתמכות בלבד.
7. העברת אפליקציה מסביבת פיתוח לייצור תתבצע בצורה מבוקרת.
8. בסביבת הפיתוח המרכזית לא נעשה שימוש בנתונים אמיתיים של הלקוחות. עם זאת, קיימת סביבת פיתוח ייעודית, המבודדת לחלוטין מרשת הייצור, שבה עשוי להיעשות שימוש בנתונים אמיתיים על בסיס צורך בלבד, לצורך בדיקה ופתרון בעיות של לקוחות שלא ניתן לשחזר בדרך אחרת. שימוש בסביבה זו מתבצע בתוך גבולות הבקורות והנהלים לאבטחת מידע שנקבעו על ידי הספק, ומוגבל בהתאם למטרה זו בלבד.
9. Minimum Security Standards for Software-as-a-Service (SaaS):  
[https://uit.stanford.edu/guide/securitystandards/saas\\_paas](https://uit.stanford.edu/guide/securitystandards/saas_paas)

אדית  
מתלונות תוכנה בע"מ  
ח. 514140605  
הספק