# נספח אבטחת מידע לכתב התחייבות לשימוש בשירותי API

# עבודה עם Refresh Token

כחלק מארכיטקטורת הרכיב יש לאפשר לצד ג' לאחסן בשרתיו את פרטי ההזדהות של לקוחותיו. (JWT TOKEN+REFRESH TOKEN)

פרטי הזדהות אלו ברמת רגישות גבוהה מאוד ודליפתם תאפשר ביצוע פעולות בשם הלקוחות ללא ידיעתם.

על מנת להגן על פרטי הזדהות אלו על החברות צד ג' להתאים את עצמם לדרישות הבאות:

## תקשורת:

* 1. כל התקשורת אל שע"מ וכן התקשורת הפנימית אצל החברה צד ג' תתמוך HTTPS בלבד בתקן TLS האחרון או אחד לפניו (נכון לכתיבת מסמך זה 1.2)

## כל ה- ciphers שבשימוש יהיו מעודכנים וללא פגיעויות ידועות. (נכון לזמן מסמל זה - כך יש להשתמש ב RSA או ECDSA 256-bit)

* 1. אם וכאשר תמצא פגיעות באחד הפרוטוקולים אזי יש לבצע עדכון גירסה תוך 30 יום, אלא אם כן מופצת הודעה אחרת משע"ם

## אחסון פרטי הזדהות (JWT+REFRESH):

## יוגדר מסד נתונים ייעודי ומופרד משאר מסדי הנתונים של הצד ג' עבור אחסון הנתונים.

## מסד הנתונים זה יהיה מוצפן בהצפנה אשר לא ידוע עליה פגיעויות קיימות. מפתחות ההצפנה ינוהלו בנפרד על ידי מנהל סיסמאות חיצוני.

## שרת מסד הנתונים יהיה מוקשח לפי הסטדנרטים הקיימים לאותה מערכת הפעלה וכן יהיה בעל עדכוני אבטחה שוטפים.

כל עדכון אבטחה ברמה "גבוהה" יש לבצע תוך 30 יום, אלא אם כן מופצת הודעה אחרת מאת שע"ם.

## ניהול המשתמשים במסדי הנתונים - יש לוודא כי יש קיימת מערכת ניהול משתמשים על מסד הנתונים וכי הגישה למסד הנתונים היא רק על ידי משתמש אפליקטיבי.

## יש לבצע AUDIT על מסד הנתונים באופן מלא וכל המידע יישמר לתקופה של 12 חודשים.

## את הלוגים יש לשמור בשרת נפרד והגישה אליהם תהיה עם משתמש ייעודי.

במצב של שימוש במערכת מקומית אשר מחייבת שמירת פרטי הזדהות על שרת הנמצא בבית העסק יש לעמוד בכל ההנחיות שלעיל ובנוסף:

1. מסד הנתונים המכיל את פרטי ההזדהות יהיה במחיצה נפרדת המוצפנת באופן עצמאי ברמה הלוגית או הפיזית. יש לוודא כי בית התוכנה ממלא אחר ההוראות של שע"ם בנושא.
2. מפתח ההצפנה יישמר במנהל סיסמאות חיצוני כאשר "המפתח הראשי" יישמר מחוץ לשרת זה.

יש להקפיד כי בית התוכנה ממלא אחר הוראות שע"ם בנושא.