review requirements

הסקר הבא מתייחס לפיצ'ר יצירת בידוד קבוצתי החדש שהוגדר למערכת, הפיצ'ר נועד לאפשר למשתמשים ליצור קבוצות בידוד עבור אנשים הנחשפים לנגיף באופן קבוצתי, כל זה במטרה לייעל את תהליך העדכונים של נתוני הבידוד בצורה טובה יותר.

1.**דרישות מצד המשתמש:**

1.1**ממשק משתמש:**

הממשק יהיה בצורה ברורה, קלה לתפעול ונעימה למשתמש.

יהיו שלוש שדות להזנת הנתונים: שדה להזנת תאריך חשיפה

שדה להזנת תאריך החלמה

אפשרות אופציונלית לבחור אנשים שנחשפו לנגיף ולהוסיף לקבוצה

זה טוב מאחר ולא תמיד ניתן להגיע לכל האנשים שנכחו במקום ע"י הנ.צ. שהתקבל במידה ולא בהכרח שיש להם יכולת להתחבר למיקום ו/או אפשרות לאתר אותם.

כאשר הנתונים מתקבלים ואחרי בדיקת תקינות, הנתונים מתווספים לבסיס הנתונים במאגר המידע.

1.2**יצירת בידוד:**

אפשרות ליצור קבוצת בידוד בהתאם לתאריך חשיפה לנגיף.

אפשרות להוסיף ולהסיר חברי קבוצה מהבידוד.

1.3**עריכת נתונים:**

בכל שלב שהוא תהיה אפשרות על המשתמש לערוך את הנתונים שכתב עם זה בתאריכים שהכניס ואם זה בהוספה ובהסרה של חברי הקבוצה.

המערכת תמיד תתעדכן בבסיס הנתונים בזמן אמת.

1.4**קבלת התראות:**

כל אדם שהוכנס לקבוצת בידוד, יקבל בזמן אמת התראה לכך בהודעת SMS בהתאם למספר הפלאפון שלו במערכת.

1.5**תקשורת:**

תהיה אפשרות ליצירת קשר עם איש קשר מטעם המערכת לכל שאלה או הסבר בהתאם.

2.**דרישות טכניות:**

2.1**אימות הנתונים:**

לפני שליחת הנתונים תקפוץ הודעה לבדיקה חוזרת של הנתונים ע"י המשתמש על מנת שישים לב שכל הנתונים נכונים ומאומתים.

כל אדם שהוכנס לקבוצת בידוד ע"י משתמש אחר, המערכת תסנכרן את הנתונים של האדם עם הנתונים הקיימים במערכת ע"מ לוודא שלא קיים סתירה בזמנים ובמיקום של אותו אחד.

2.2**שילוב טכנולוגי:**

שילוב של ממשק GOOGLE MAPS ע"י שימוש בAPI של GOOGLE MAPS על מנת לקבל נתונים גיאוגרפים של המיקום ולהציגם במפה.

שילוב נתונים של מערכת הטלפונים הציבורית ע"מ לזהות אנשים שנחשפו לנגיף במקום מסוים, זה יכול להיעשות דרך API או דוא"ל ליצירת קשר ישיר עם המערכת.

2.3**ניהול שגיאות:**

במקרה של שדות ריקים תקפוץ הודעה של חסר ולא יהיה ניתן להשלים את השליחה ללא מילוי השדה.

גם המקרה של מידע לא תקין או לא מסונכרן תקפוץ הודעת שגיאה.

2.4**אבטחת מידע:**

תהיה אבטחה מוצפנת מקצה לקצה של נתוני המשתמשים ונתוני הבידוד במערכת.

מנגנון אבטחה למניעת גישה לא מורשית למידע רגיש.

יהיו רמות גישה שונות, כלומר לדוגמא המנהלים יוכלו לגשת לכל המידע בעוד שמשתמשים רגילים לא יוכלו לגשת למידע שלא קשור אליהם.

לפני קבלת מידע כלשהו ממשתמשים, תהיה בדיקת הסכמה מלאה מצד המשתמש לכך בהתאם לתקנון הפרטיות ולתנאי השימוש במערכת.

אחת לתקופה תהיה בדיקת אבטחה מערכת כוללת לשמירת אבטחת הנתונים הקיימים.

2.5**בדיקות ואימות:**

לפני הפצת הפיצ'ר ייעשו בדיקות מקיפות של אימות ותקינות הפיצ'ר.

בדיקת יכולת המערכת לטפל בתעבורה רבה ולפעול ביעילות בכל מצב.

נרצה שהמערכת תשים דגש ותוכל לטפל בכל מיקרה קצה שתיתקל בו בצורה טובה ויעילה.

2.6**תיעוד:**

תיעוד מפורט של כל התהליכים והפונקציונאליות של המערכת עם הפיצ'ר.

תיעוד טכני לכל רכיב במערכת ולתהליכי עבודה.