נספח דרישות אבטחת מידע

1. עקרונות כלליים

- ציות לתקנות: הספק נדרש לעמוד בחוק הגנת הפרטיות (תיקון 13) ובתקנות אבטחת המידע של נתיבי איילון.
- הגדרת מידע רגיש: כל מידע יוגדר כרגיש ויאובטח בהתאם לעקרונות CIA - Confidentiality, Integrity, Availability..
- עמידה בדרישות סייבר: כל רכיב, ממשק או שירות חייב לעמוד בדרישות אבטחת המידע של נתיבי איילון, כולל בקרה, ניטור ודיווח.

2. הגנה על תעבורת נתונים וממשקים

- הצפנה בתעבורה: כל העברת נתונים בין רכיבי המערכת לענן של נתיבי איילון תתבצע בפרוטוקול מוצפן (TLS 1.3 או גרסה עדכנית).
- הצפנה בנתונים: נדרש שימוש במנגנוני הצפנה at-rest ו-in-transit (AES-256 לפחות).
- ממשקים מאובטחים: הממשקים (API/Web) יוגדרו על בסיס עקרונות Zero Trust, עם אימות רב-שלבי (MFA) והרשאות מבוססות תפקיד (RBAC).
- ניהול מפתחות: מפתחות הצפנה ינוהלו באמצעות מנגנון KMS של AWS.

3. אחסון וניהול מידע

- מיקום אחסון: כל המידע יאוחסן אך ורק בענן AWS של נתיבי איילון. אין לשמור עותקים מקומיים לאחר קבלת אישור קליטה בענן.
- מדיניות שמירת מידע: יש להגדיר Data Retention Policy למחיקה אוטומטית של נתונים לאחר תקופה שתוגדר.
- טשטוש מידע מזהה: יש לבצע טשטוש נתונים מזהים (כגון פנים ולוחיות רישוי) לפני העברה ואחסון, בהתאם לדרישות החוק.
- תיעוד גישה: יש לשמור תיעוד מלא (Audit Logs) של כל ניסיון גישה, שינוי או מחיקה.

4. בקרות גישה והרשאות

- ניהול הרשאות: יש להשתמש במנגנון IAM לניהול הרשאות.
- עקרון מינימום הרשאה: גישה תינתן לפי עקרון Least Privilege – הרשאות מינימליות בהתאם לצורך.
- אימות משתמשים: נדרש שימוש ב-MFA לכלל המשתמשים, כולל טכנאים חיצוניים.
- ניתוק אוטומטי: יש להפעיל מנגנון Session Timeout לניתוק אוטומטי לאחר חוסר פעילות.

5. אבטחת תשתיות ותחנות קצה

- בידוד רשתי: ציוד הקצה יחובר לרשתות מבודדות כדי למנוע גישה לא מורשית.
- חיבור מאובטח: חיבורי התקשורת יתבצעו באמצעות VPN/IPSec מאובטח מול נתיבי איילון.
- ניהול עדכונים: הספק יבצע Patch Management שוטף לכל רכיבי התוכנה והחומרה.
- הגנת תחנות קצה: נדרש מנגנון Endpoint Protection (EDR) בתחנות עיבוד מקומיות, הכולל אנטי-וירוס וזיהוי אנומליות.

6. ניטור, גילוי ודיווח

- חיבור למערכות ניטור: הספק חייב לחבר את כל הלוגים והאירועים למערכת ה-SIEM של נתיבי איילון או למערכת ניטור חלופית אחרת אשר תאושר מראש ע"י גורמי אבטחת המידע בנתיבי איילון.
- ניטור תעבורה: יש להפעיל מערכות IDS/IPS לניטור תעבורת נתונים.
- דיווח אירועים: כל אירוע אבטחה/סייבר ידווח תוך 4 שעות לכל היותר.
- בדיקות תקופתיות: יש לבצע בדיקות חדירה (PT) ו-Risk Assessments לפחות אחת לשנה.

7. המשכיות עסקית והתאוששות מאסון (BCP/DRP)

- גיבוי ושחזור: נדרש גיבוי יומי של כל הנתונים לענן של נתיבי איילון, עם בדיקות שחזור תקופתיות.
- זמינות שירות: נדרשת זמינות של 99.9% לפחות.
- זמן התאוששות: במקרה של תקלה קריטית, יש לחזור לפעילות מלאה תוך 24 שעות.

8. ניהול ספקים וצד ג'

- הסכמי סודיות: כל ספק משנה יחתום על הסכם DPA (הסכם לעיבוד מידע) עם התחייבות לאבטחת מידע.
- איסור העברת מידע: אין להעביר מידע מחוץ לישראל ללא אישור בכתב.
- ביקורת ספקים: יש לבצע ביקורת ספקים שנתית.

9. תקנים וציות

- תקנים בינלאומיים: ספק המערכת יעמוד בתקנים ISO/IEC 27001, 27017, 27018 (ענן).
- ניהול פרטיות: עמידה בתקן ISO 27701.
- עמידה במסגרת ה-NIST Cybersecurity Framework.
- התחברות ל-SOC: עמידה מלאה בדרישות אבטחת המידע של נתיבי איילון, כולל חיבור ל-SOC (מרכז תפעול אבטחה).