**דרישות אבטחת מידע – ISP**

1. כל רכיבי המערכת יעברו בדיקות חדירות/חוסן וסקר קוד.
2. הפתרון ימומש בתצורת Front/Back עם הפרדה מלאה לשלוש שכבות (3 Tier) תצוגה, BL, מסד נתונים. אם נדרש רכיב ניהול הוא יבנה בנפרד בצד האחורי של המערכת.
3. שימוש בקוד צד ג' כמו plugin, מחלקות עזר, מוצרי משלימים וכו' דורש אישור מראש בדיקות חדירות וסקר קוד.
4. אין להשתמש ברכיב IFRAME בתוך הפתרון. אם יש צורך להציג מידע מאתר אחר הדבר יתבצע באמצעות פתיחת דף נפרד.
5. כל מקום באתר בו מוצג מידע מצד ג' יסומן בצורה ברורה עם כיתוב "המידע המוצג מגיע מאתר X".
6. לא תתאפשר גישה לשירותים ברשת אינטרנט מצד השרת (server side).
7. הפתרון יתמוך בהזדהות עם כרטיס חכם ו/או SSO על פי הנחיות ה-ISP.
8. הטמעת web service בתוך הפתרון תעשה על פי תקן ws.gov.il
9. הגישה לשרתים תתבצע ממתקני ה-ISP עצמו. לא תתאפשר גישה מרוחקת לשרתים או לחלקי המערכת.
10. כל שינוי במערכת מהווה "גירסה" ועליו לעבור בדיקות חדירות וסקר קוד.
11. טיפול בממצאי סקר קוד/בדיקת חוסן – יש לטפל בכל הממצאים לפני קבלת אישור עליה לאויר.
12. כל רכיבי הפתרון יתארחו ב-ISP. אין להשתמש בפתרונות מבוססי ענן פומבי.
13. דפים בהם מתבקש המשתמש למלא פרטים יכילו רכיב captcha ויהיו מוגנים ב-SSL.
14. הפתרון יספק לוגים מפורטים על פעילות משתמשים ותהליכים מעבר ללוגים המגיעים כברירת מחדל עם מערכת ההפעלה או המוצר התשתיתי.
15. שימוש בפרוטוקול Rest ו- Jeson יתבצע לצורך קריאה בלבד (GET)
16. יש לעמוד במדיניות ההקשחה של ממשל זמין .
17. יש לעמוד בהנחיות פיתוח מאובטח עבור מערכות המאוכסנות