דף הנחיות למבקר: ביקורת אתר האינטרנט של הרשות/התאגיד

מטרת הביקורת: בחינת רמת אבטחת המידע (Cyber Hygiene), עמידה בחוק הגנת הפרטיות ועמידה בחובות הפרסום המוטלות על רשויות ציבוריות.

א. בדיקת תקינות הצהרת פרטיות

מה בודקים: עמידה בחוק הגנת הפרטיות ותקנותיו (חובה חקוקה לרשות ציבורית).

1. חפש באתר את הקישור "מדיניות פרטיות" או "תנאי שימוש" (לרוב בתחתית הדף).
2. העתק את נוסח המדיניות במלואו.
3. **הנחיה למבקר:** גש ל-AI והזן את הפקודה: *"להלן הצהרת הפרטיות באתר של רשות מקומית XX. בחן את עמידתה בהוראות החוק (מטרת האיסוף, זכות העיון, אבטחת מידע) וציין ליקויים".*
4. **ניתוח תוצאות:** העדר הצהרה או הצהרה שאינה מפרטת את זכויות העיון והתיקון של התושב מהווה הפרה של חוק הגנת הפרטיות.

ב. בדיקת ציות לחובות פרסום (סעיף 2ב48 לפקודה)

מה בודקים: האם הרשות שקופה ומפרסמת את כל המידע שהחוק מחייב (פרוטוקולים, תקציב, חוקי עזר).

1. הורד את חוברת "חובות פרסום באינטרנט" (של משרד המשפטים/היחידה לחופש המידע).
2. העלה את הקובץ ל-AI.
3. **הנחיה למבקר:** הזן את הפקודה: *"בדוק את עמידת האתר [כתובת URL] בהוראות המופיעות במסמך המצורף. בדוק במיוחד פרסום פרוטוקולים, הקלטות ישיבות, חוקי עזר ופרטי ממונה חופש המידע".*
4. **ניתוח תוצאות:** אי-פרסום פרוטוקול במועד (תוך יומיים מאישורו), או חוסר בהקלטות ישיבות מהווה חריגה מהוראות פקודת העיריות/המועצות המקומיות.

ג. בדיקת הצפנה ואבטחת חיבור (HTTPS / SSL)

מה בודקים: האם התקשורת בין התושב לאתר מוצפנת והאם נעשה שימוש בפרוטוקולים עדכניים.

1. היכנס לאתר: SSL Labs - SSL Test.
2. הזן את כתובת האתר של הרשות.
3. המתן לסיום הסריקה וקבלת הציון (A-F).
4. **ניתוח תוצאות:** ציון נמוך מ-A מעיד על שימוש בפרוטוקולים מיושנים (כמו TLS 1.0) או תעודה פגת תוקף, החושפים את המשתמשים לגניבת מידע.
5. **הנחיה למבקר:** העתק את סיכום הממצאים, הדבק ב-AI (Gemini/ChatGPT) ובקש: *"כתוב פרק לדוח ביקורת המנתח את ממצאי ה-SSL הללו והשפעתם על אבטחת המידע ברשות".*

ד. בדיקת כותרות אבטחה (Security Headers)

מה בודקים: הגנות מובנות בדפדפן המונעות התקפות נפוצות (כגון Clickjacking או XSS).

1. היכנס לאתר: Security Headers.
2. הזן את כתובת האתר ולחץ על Scan.
3. **ניתוח תוצאות:** הדירוג משקף כמה "שכבות הגנה" הוגדרו בשרת. חוסר ב-Headers (כמו CSP או HSTS) מקל על תוקפים להזריק קוד זדוני לאתר.
4. **הנחיה למבקר:** העתק את רשימת הכותרות החסרות, הדבק ב-AI ובקש: *"להלן תוצאות בדיקת Security Headers לאתר הרשות. נתח את המשמעות של הכותרות החסרות עבור דוח ביקורת סייבר".*

ה. הפקת דוח ביקורת מסכם

לאחר סיום כלל הבדיקות ואיסוף ניתוחי ה-AI, על המבקר לגבש את הממצאים למסמך אחד.

הנחיה למבקר: פנה ל-AI בפקודה הבאה:

"רכז את כל הממצאים שאספנו (SSL, כותרות אבטחה, פרטיות וחובות פרסום) לכדי טיוטת דוח ביקורת פנימית עבור המועצה המקומית/החברה הכלכלית. חלק את הדוח ל: תקציר מנהלים, פירוט ממצאים לפי סעיפים, הערכת סיכונים והמלצות לתיקון."

דגש למבקר: יש לוודא כי הבדיקות מבוצעות על האתר הרשמי בלבד, ולשים לב כי עבור חברות כלכליות או מרכזים קהילתיים, חובות הפרסום עשויות להשתנות (חוק חופש המידע חל עליהם כ"גוף ציבורי" אך סעיפי פקודת העיריות חלים בעיקר על הרשות עצמה).