הנחית רשם גורמים מאשרים מס' 2/2015

חוות דעת של מבקר גורם מאשר

1. מטרות

1.1 מטרת הנחייה זו לפרט את התנאים הנדרשים להתקיים בחוות דעת של מבקר, המוגשת בהתאם לתקנה 2(8) לתקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב-2001 (להלן – **תקנות רישום וניהול**) לגבי מערכות גורם מאשר שנרשם במרשם הגורמים המאשרים לפי חוק חתימה אלקטרונית, התשס"א-2001 (להלן - **החוק**), כולל כל גורם רושם או אחר הפועל עבורו או מטעמו (להלן - **הגורם המאשר**).

1.2 לפרט את התנאים הנדרשים להתקיים במבקר העורך חוות דעת מבקר כאמור (להלן - **המבקר**).

2. רקע

2.1 תקנה 2(8) לתקנות רישום וניהול מחייבת הגשת "חוות דעת של מבקר לפי כללי ביקורת מקובלים בדבר נאותות מערכות המידע, מערכות הבקרה ואמצעי האבטחה... והכל להנחת דעתו של הרשם".

2.2 בנוסף, בתקנה 2(8) לתקנות רישום וניהול מפורטות הדרישות אותן נדרש לקיים המבקר לצורך קיום חובה זו, כאשר הובהר בסיפא לס"ק (ה) כי "הכל להנחת דעתו של הרשם".

2.3 הנחית הרשם מספר 2/2010 בנושא תקן מקובל למערכת ניהול תעודות אלקטרוניות בגורם מאשר מפרטת את הדרישות לעניין מהות הבדיקה שיש לערוך בחוות הדעת, כולל הפניה לתקן CWA 14167-1.

3. הנחיה

3.1 הביקורת שעורך המבקר נועדה לבדוק האם כל מערכות המידע המשמשות את הגורם המאשר, לרבות אמצעי הבקרה והאבטחה המשולבים בהן, מקיימות את הוראות החוק ותקנותיו המפורטות בנספח א' להנחיה זו, וכן האם אמצעי בקרה ואבטחה אלו מופעלים ומיושמים כראוי על ידי הגורם המאשר.

3.2 הנחייה זו מבטלת ומחליפה את הנחיית רשם 6/2004 "חוות דעת של מבקר".

3.3 <u>המבקר וצוות הבדיקה</u>

3.3.1 על המבקר להיות להנחת דעת הרשם כמפורט בתקנה 2(8) לתקנות רישום וניהול.

3.3.2 הנחיית הרשם 2/2010 גם מפנה לתקן העזר CWA-14172 לעניין הדרישות החלות על המבקר או על צוות הביקורת אשר הינו להנחת דעתו של הרשם. בפרט, סעיף 3.3 להנחיה מדגיש כי על המבקר להיות בעל "ניסיון מעשי בתחום ה-PKI להנחת דעתו של הרשם", שכן תחום ה - PKI מהווה את הליבה של תשתיות אבטחת מידע בגורם המאשר.

3.3.3 בנוסף, על המבקר לעמוד בתנאי הכשירות והניסיון המקצועי כמפורט בתקן CWA 14172-2, ותקן CWA 14172-3 על מנת להניח את דעתו של הרשם כאמור בתקנה 2(8) לתקנות רישום וניהול.

3.3.4 כל הבדיקות חייבות להתבצע על ידי אנשי מקצוע בעלי מומחיות, כאשר צוות הבדיקה חייב לכלול גם מומחים לאבטחת מידע עם ניסיון תקיפה מוכח וניסיון בתחום PKI.

3.4 <u>עריכת הבדיקות</u>

3.4.1 בהתאם להנחיית הרשם 2/2010, עריכת הבדיקה על מערכות הגורם המאשר מחייבת שילוב של בדיקה נוהלית תפעולית עם בדיקה של מערכות ספציפיות שמותקנת בגורם המאשר, תוך התייחסות לסיכונים הקונקרטיים שיש לגורם המאשר הספציפי בהתאם לקווים המנחים בתקן CWA-14167 ולהתמודדות עם סיכונים אלה. על הבדיקה להתבצע לפי הכללים הקבועים בתקן העזר CWA-14172.

3.4.2 ביצוע הבדיקות ייגמר בטווחי זמן סבירים, ובתנאי שלא יבוצעו שינויים במערכת בין הבדיקות, שאינן על דעת המבקר ושלא הובאו לידיעתו, והדבר אף יצוין בדוח הביקורת המפורט.

3.4.3 הבדיקות תכלולנה את כל אלה:

3.4.3.1 בדיקת קיום, שלמות ועדכניות תיעוד "תיק אתר" הכולל: תרשימי רשת, חומרה עדכנית כולל רכיבי רשת, שרתים ותחנות, גרסאות תוכנה של כל הנ"ל, תיעוד התקנות, חוקי כלי אבטחה, זרימת פרוטוקולים ותיעוד הגדרות כלי רשת;

3.4.3.2 בדיקת אמצעי האבטחה הפיזית בכל מתקני הגורם המאשר;

3.4.3.3 סקירה על מדיניות האבטחה ומידת הטמעתה אצל העובדים בארגון;

3.4.3.4 בדיקת הקשחות מלאה, הן ברמות מערכות ההפעלה, תוכנות התשתית והיישומים השונים, כולל בדיקות התקנת עדכוני יצרן וטלאי אבטחת מידע;

3.4.3.5 בדיקת כלי האבטחה כגון: AV, IPS, FW, בדיקת מדיניות החוקים ובדיקת אפקטיביות החוקים;

3.4.3.6 בדיקת מערכות התחזוקה (maintenance) האמורות להבטיח המשך עדכונים בצורה מאובטחת (ללא גישה ישירה לאינטרנט);

3.4.3.7 בדיקת מערכת השו"ב, בדיקת מדיניות ובדיקת אפקטיביות;

3.4.3.8 בדיקת מערכת איסוף וניתוח הלוגים, בדיקת מדיניות ובדיקת אפקטיביות;

3.4.3.9 סקר סיכונים לכל מערכות המידע המשמשות את הגורם המאשר וכן בדיקות חדירות לאחר סיום כל העבודה כאמור בסעיפים 3.7 ו-3.8 להלן;

3.4.3.10 בדיקת קוד (Code Review) לפיתוחים עצמאיים שאינם חלק מהתוכנה שנרכשה וקבצי התיעוד לבדיקות;

3.4.3.11 בחינת צורך בשדרוג מערכות קיימות במערכות חדשות בעלות רמת אבטחה גבוהה יותר או ברכישה והטמעה של מערכות אבטחת מידע שאינן קיימות במערכות המידע המשמשות את הגורם המאשר;

3.4.3.12 בחינת אירועי אבטחת מידע בתחום ה- PKI וה- CA שהתפרסמו והסקת מסקנות לגבי יכולת התמודדות הגורם המאשר באירועים מסוגים אלו (לדוגמה אירוע diginotar).

3.4.4 לצורך הבדיקות רשאי המבקר להסתמך על דו"ח מעבדה מוסמכת המעיד על התאמת מערכת מבוקרת לתקן CC או תקן מקובל אחר להנחת דעתו של הרשם ובלבד שאימת את ההנחות המפורטות בדו"ח הבדיקה לגבי אופן השימוש במערכת.

3.5 <u>דוח ביקורת מפורט</u>

3.5.1 דוח ביקורת מפורט ייערך לפי המבנה שלהלן:

3.5.1.1 תיאור גבולות הגזרה של הבדיקה בהתאם לסיכונים הקיימים בגורם המאשר, ועומק הבדיקה שהתבצעה בהתאם לתוחלת כל סיכון. אם ישנו רכיב שלא נכלל בגבולות הגזרה של הבדיקה, על המבקר לנמק את הסיבה לכך. כאשר מדובר ברכיב של צד שלישי מוכר, ניתן להתבסס על אסמכתאות מהליך תקינה או תיעוד אחר ככל שהן מקובלות;

3.5.1.2 פירוט באופן מדויק של מכלול רכיבי המערכת שנבדקו, לצד תיאור הארכיטקטורה של המערכת. ככל שמדובר בנתונים סטנדרטים הקשורים לרכיב המופיע בתיעוד של המוצר (כגון נתונים על אופן פעולת מערכת ההפעלה), ניתן להסתפק בהפניה קצרה יותר.

3.5.2 לגבי כל בדיקה שבוצעה יש לפרט:

3.5.2.1 הנושא הנבדק;

3.5.2.2 סעיף בתקן, בחוק או בתקנות ו/או במבחני הרשם;

3.5.2.3 המערכת הנבדקת;

3.5.2.4 תהליך הבדיקה, כולל מפרט הפעולות שבוצעו ותיאור הכלים שאיתם בוצעו הפעולות;

3.5.2.5 צילומי מסך של הנושא הנבדק;

3.5.2.6 לוגים ותיעוד רלוונטי של המערכות הנבדקות;

3.5.2.7 ממצאי הבדיקה;

3.5.2.8 הליקוי שנמצא והתיקון שבוצע לגביו, או הערכת הזמן ומשאבים הנדרשים לתיקון, והבקרה המפצה בתקופה זו;

3.5.2.9 רמת חשיבות/סיכון ;

3.5.2.10 סטטוס במועד הגשת הדוח ;

3.5.2.11 במקרה בו דרישת האבטחה שבתקן CWA-14167-1 לא מתקיימת ברכיב מסוים במערכות הגורם המאשר, על המבקר לפרט את הפערים בין הרכיב לבין דרישת האבטחה בתקן. ככל שישנם פערים, יש לפרט כיצד הגורם המאשר מגשר על פערים אלו תוך מתן הסבר הגיוני המניח את הדעת.
יובהר, כי בכל מקרה תינתן עדיפות לכך שהיישום של הדרישה בתקן יתקיים ברכיב עצמו ;

3.5.2.12 תאריך בדיקה ;

3.5.2.13 נבדק ע"י (שם המבקר) ;

3.5.2.14 אושר ע"י (נציג הגורם המאשר).

3.6 <u>כללי ביקורת מקובלים</u>

3.6.1 תקנים, הנחיות ונהלים לעריכת ביקורת מערכות מידע שפורסמו ע"י אחד מבין הגופים המפורטים להלן יהוו "כללי ביקורת מקובלים" כנדרש בתקנה 2(8) לתקנות רישום וניהול ;

3.6.1.1 לשכת רואי החשבון בישראל ;

3.6.1.2 ISACA - Information Systems Audit and Control Association ;

3.6.1.3 ICS2– International Information Systems Security Certification Consortium Inc

3.6.2 בביצוע הביקורת ניתן להיעזר גם בפרסומים הבאים :

3.6.2.1 מדריך SP 800-115 של NIST "Technical Guide to Information Security Testing and Assessment" ;[1]

3.6.2.2 מסמך Open Source Security Testing Methodology Manual (OSSTMM) מאת ארגון ISECOM ;[2]

3.6.2.3 BSI-Standard 100-3 של משרד אבטחת המידע הפדרלי בגרמניה "Risk Analysis based on IT-Grundschutz" ;[3]

[1] בקישור : http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
[2] בקישור : http://www.isecom.org/research/osstmm.html
[3] בקישור :

3.6.2.4 "BSI - Study A Penetration Testing Model" של משרד אבטחת המידע הפדרלי בגרמניה[4].

3.7 <u>סקר סיכונים</u>

3.7.1 על סקר סיכונים להתייחס לכל הנושאים הבאים:

3.7.1.1 פירוט כל הנכסים עליהם יש להגן (כגון: מפתחות, תעודות, פרטים אישיים של מונפקים, אובייקטים שונים במערכות ההפעלה וביישומים השונים, בסיסי הנתונים, מערכי אחסון, רשת וציודי התקשורת ורכיבי האבטחה השונים);

3.7.1.2 פירוט האיומים השונים העומדים בפני הגורם המאשר, רמת הסכנה הנשקפת למידע בכל איום שהתגלה, וכיצד הגורם המאשר מתמודד עם כל איום שכזה;

3.7.1.3 פירוט תוצאות בדיקות, הן ידניות והן של כלי האבטחה השונים בהם התבצע שימוש לצורך הבדיקות, מפרט הקשחות של רכיבי רשת, שרתים ומסדי-נתונים;

3.7.1.4 תיאור מפרטי ביצוע ותוצאות בדיקות חדירות פנימית וחיצונית בשיטות קופסא שחורה וקופסא לבנה.

3.7.2 את הסקר יש לממש גם באמצעות כלים, ביחוד בבדיקות ההקשחה ובדיקות התקנת הטלאים המומלצים. כל הבדיקות שתעשינה, לרבות אלו המציגות תוצאות חיוביות תתועדנה באופן מלא.

3.8 <u>בדיקות חדירות</u>

3.8.1 בדיקות החדירות תבוצענה על הרשת הפנימית ועל הרשת החיצונית של הגורם המאשר וכן בדיקות מחוץ לרשת הגורם המאשר.

3.8.2 בדיקות החדירות תכלולנה שני סוגי בדיקות: בדיקה כללית ואוטומטית לזיהוי בעיות אבטחת המידע ובדיקה יסודית וידנית לאיתור חשיפות שונות בשירותים הפעילים בגורם המאשר;

3.8.3 על הבדיקה הידנית לכלול את האפשרות הפוטנציאלית לביצוע, בין היתר, את הנושאים הבאים:

3.8.3.1 עקיפת מערכות ההגנה מסוגים שונים;

3.8.3.2 עקיפת מנגנוני ההזדהות ופיצוח סיסמאות;

---

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile

[4] בקישור:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile

3.8.3.3 השתלטות על מערכות ברשת הארגון והחדרת קוד עוין לתוך הארגון ;

3.8.3.4 ביצוע Social Engineering להשגת מידע מעובדי הארגון ;

3.8.3.5 אפשרות לחדירה פיזית לתוך הארגון.

3.9 <u>חוות דעת המבקר</u>

3.9.1 חוות דעת המבקר תהיה ערוכה בהתאם לטופס המצוי בנספח ב', תישא תאריך חתימה עדכני אשר הפרש הימים בינו ובין תאריך ההגשה אינו עולה על שבועיים.

3.9.2 לחוות הדעת יצורפו :

3.9.2.1 דוח ביקורת מפורט, לפי כל המפורט לעיל ;

3.9.2.2 דוח סקר סיכונים, לפי כל המפורט לעיל ;

3.9.2.3 דוח מבדקי חדירות לפי כל המפורט לעיל ;

3.9.2.4 טופס הסכמה לקבלת מידע מהמרשם פלילי והצהרה על העדר כתב אישום חתום ומאומת על ידי עורך דין (ר' נספח ג' להנחיה).

3.9.3 חוות הדעת תסכם את תוצאות דוח הביקורת המפורט, ותכלול מסקנת המבקר לאור תוצאות אלה כי מערכות הגורם המאשר נאותות ומהימנות.

3.10 יודגש, כי ההחלטה הסופית בעניין קבלת חוות הדעת ודוחות הביקורת הינה של הרשם.

אלון בכר

ראש הרשות למשפט, טכנולוגיה ומידע
רשם גורמים מאשרים

נספח א' – הוראות חוק ותקנות הרלבנטיות לביקורת

מס' סעיף/תקנה	חיקוק	הנושא
18(ד)	חוק חתימה אלקטרונית	מערכות חומרה ותוכנה מהימנות
3	תקנות חומרה ותוכנה[5]	זמינות מערכת לבדיקת תוקף תעודות
4	תקנות חומרה ותוכנה	אבטחת אמצעי חתימה של הגורם המאשר
5(א)	תקנות חומרה ותוכנה	עמידת מרכיבי המערכת בתקן CC או תקן מקובל אחר
5(ב)	תקנות חומרה ותוכנה	אבטחת אמצעי התקשורת
7(א)	תקנות חומרה ותוכנה	הפרדת תפקידים
7(ב)	תקנות חומרה ותוכנה	בקרת גישה
7(ג)	תקנות חומרה ותוכנה	זיהוי ותיעוד גישה
13	תקנות רישום וניהול[6]	איסור החזקת אמצעי חתימה בידי הגורם המאשר
14	תקנות רישום וניהול	שימוש בשפה העברית
15(ב)	תקנות רישום וניהול	אבטחת מאגרי נתונים
15(ג)	תקנות רישום וניהול	זמינות מאגרי תעודות
19	תקנות רישום וניהול	מערכת לניהול תצורה
19	תקנות רישום וניהול	רישום פעולות ואירועים
20	תקנות רישום וניהול	גיבוי ושמירה

[5] תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001.

[6] תקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב- 2001.

<u>נספח ב' - חוות דעת של מבקר</u>

בהתאם לתקנה 2(8) לתקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב- 2001

אני הח"מ, _____, נתבקשתי ע"י _____ (להלן: "הגורם המאשר") לחוות דעתי בנוגע למערכות המידע של הגורם המאשר ואמצעי הבקרה והאבטחה המשולבים בהן, בהתאם לתקנה 2(8) לתקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב- 2001.

הריני להצהיר כי איני ממלא משרה או בעל עניין כל שהוא בגורם המאשר, ואיני קרוב משפחה מדרגה ראשונה של הגורם המאשר או מנהל הגורם המאשר. כמו כן הנני מצרף לחוות דעתי טופס הסכמה לקבלת מידע מהמרשם הפלילי להוכחת עמידתי בדרישת תקנה 2(8)(ג) לתקנות חתימה אלקטרונית הנ"ל.

להלן פרטיי השכלתי והכשרתי המקצועית:
(אנא פרט: השכלה אקדמית, תארים, הכשרה בביקורת מערכות מידע וצרף אסמכתאות)

_____
_____
_____
_____
_____

להלן פרטי ניסיוני המקצועי בתחום ביקורת מערכות מידע:

_____
_____
_____
_____
_____

ערכתי את ביקורתי לפי כללי ביקורת מקובלים כדלקמן:

_____
_____
_____
_____

על סמך הביקורת שערכתי הריני לחוות דעתי כדלקמן:

_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
_____
_____

מצורפים דו"ח הביקורת המפורט, דוח סקר הסיכונים, דוח מבדקי החדירות והמסמכים הנוספים שעליהם מבוססת חוות דעתי לעיל.

שם מלא: _____ תואר: _____ מספר רישיון: _____

כתובת: _____ תאריך: _____ חתימה: _____

<u>נספח ג': הסכמה לקבלת מידע מהמרשם פלילי והצהרה על העדר כתב אישום</u>

אני, _____ בעל תעודת זהות שמספרה: _____
שם ושם משפחה של המצהיר מספר ת.ז. כולל ספרת ביקורת
מבקר מערכות המידע

תאריך לידה: _____ שם האב: _____ ארץ לידה: _____

שם החברה/עסק: _____

1. אני החתום מטה, נותן הסכמתי לכך, שרשם גורמים מאשרים, הפועל מכוח חוק חתימה אלקטרונית, התשס"א-2001 , יקבל, בכל עת ולפי דרישתו, פרטים אודותיי מהמרשם הפלילי המנוהל על פי חוק המרשם הפלילי ותקנת השבים, התשמ"א-1981.

2. אני החתום מטה, מצהיר בזה, שלמיטב ידיעתי, לא הוגש נגדי כתב אישום ולא הורשעתי בעבירות המפורטות להלן:

2.1. עבירה מסוג "פשע" לפי הגדרתה בסעיף 24(1) לחוק העונשין, התשל"ז-1977.

2.2. עבירות לפי סעיפים 117 עד 120, 214(א), 251, 287 עד 288, 352, 418, 420, 422, 424, 430 עד 432, 445, 463, 467, 487 עד 488, ו- 496 לחוק העונשין, התשל"ז-1977.

2.3. עבירות לפי סעיפים 5, 31א לחוק הגנת הפרטיות, התשמ"א- 1981.

2.4. עבירות לפי סעיפים 3 עד 5 לחוק המחשבים, התשמ"ה- 1995.

2.5. עבירות לפי סעיפים 52ד ו- 53(א) לחוק ניירות ערך, התשכ"ח- 1968.

2.6. עבירה לפי סעיף 6 לחוק איסור לשון הרע, התשכ"ה- 1965.

2.7. עבירות לפי סעיף 81ג לחוק ההוצאה לפועל, התשכ"ז- 1967.

2.8. עבירות לפי סעיף 16 לחוק שיקים ללא כיסוי, התשמ"א- 1981.

2.9. עבירות לפי סעיף 30 לחוק חוקרים פרטיים ושירותי שמירה, התשל"ב- 1972.

3. אני החתום מטה, מצהיר בזה, כי איני תאגיד.

4. אני החתום מטה, מצהיר בזה, כי אני תושב ישראל.

_____ _____
תאריך חתימה חתימה

<u>אישור עו"ד</u>

אני הח"מ, עורך דין _____ מאשר בזה כי _____ המוכר/ת לי אישית / שזיהה/תה עצמו/ה בפני בתעודת זהות שמספרה _____, לאחר שהזהרתיו/ה כי עליו/ה להצהיר את האמת וכי יהיה/תהיה צפוי/ה לעונשים הקבועים בחוק אם יעשה/תעשה כן, אישר/ה את נכונות הצהרתו/ה דלעיל.

תאריך: _____ שם עורך הדין: _____

חתימת עורך הדין: _____

חותמת עורך הדין: _____

מספר רישיון עריכת דין: _____

מען עורך הדין: _____

מידע לגבי ההנחיה

1. **מס' ההנחיה: 2/2015**
2. **נושא ההנחיה**: חוות דעת של מבקר גורם מאשר
3. **תאריך פרסום**: 29/01/2015
4. **בתוקף מתאריך**: 29/01/2015
5. **חקיקה שאוזכרה**:
   א. חוק חתימה אלקטרונית, התשס"א- 2001
   ב. חוק המרשם הפלילי ותקנת השבים, התשמ"א- 1981
   ג. חוק העונשין, התשל"ז- 1977
   ד. חוק הגנת הפרטיות, התשמ"א- 1981
   ה. חוק המחשבים, התשמ"ה- 1995
   ו. חוק ניירות ערך, התשכ"ח- 1968
   ז. חוק איסור לשון הרע, התשכ"ה- 1965
   ח. חוק ההוצאה לפועל, התשכ"ז- 1967
   ט. חוק שיקים ללא כיסוי, התשמ"א- 1981
   י. חוק חוקרים פרטיים ושירותי שמירה, התשל"ב- 1972
   יא. תקנות חתימה אלקטרונית (רישום גורם מאשר וניהולו), התשס"ב- 2001
   יב. תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב- 2001
6. **פסקי דין שאוזכרו**: אין.
7. **מאמרים שאוזכרו**: אין.
8. **הנחיות היועץ המשפטי לממשלה שאוזכרו**: אין.
9. **הנחיות רשם מאגרי המידע שאוזכרו**:
   א. 6/2004 חוות דעת של מבקר
   ב. 2/2010 תקן מקובל למערכת ניהול תעודות אלקטרוניות בגורם מאשר.
10. **מילות מפתח**: אבטחה, בדיקות חדירות, גורם מאשר, הקשחות, חוות דעת, חתימה אלקטרונית, מבקר מערכות מידע, מערכות מידע, נהלים, סקר סיכונים, רישום.
11. **עדכונים**

גרסה	פרטים	תאריך