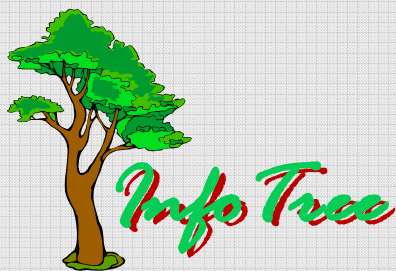




לקוח נכבד,  
7799, תקן אבטחת המידע, שיצא מבית התקנים הבריטי BSI, אומץ ע"י ISO ותופס תאוצה כתקן המוביל לאבטחת המידע. ארגונים רבים בארץ ובעולם עוברים הסמכה לקבלת תקן זה עקב דרישות פנים ארגוניות, דרישות ספקים או דרישות לקוחות. גם מכרזים גדולים בכל רחבי העולם דורשים מחברות שיעמדו בתקן זה כחלק מתנאי המענה למכרז.  
תקן 7799 אומץ בחלקו ע"י חברות הביטוח בעולם על מנת להצביע על מוכנות הארגון מבחינת אבטחת המידע.  
חברת סקיריטרי מתמחה בהכנת חברות להסמכה בתקן 7799. זאת ע"י קבוצה העוסקת בתחום המתודולוגיה המנוהלת ע"י מירב ורד, אשר עברה הכשרה בלונדון ע"י BSI להסמכה בתקן זה. מירב נחשבת כמובילה בתחום זה בארץ ובעולם. אנו מציעים את יכולת ההכנה להסמכה לתקן זה לקהל הלקוחות.  
בהמשך, מצורף המאמר "תקן ישראלי לאבטחת מידע ת"י 7799" להעשרת הידע בנושא. לקבלת פרטים נוספים ופניות בנושא, ניתן ליצור עימנו קשר בכתובת [Info@securitree.co.il](mailto:Info@securitree.co.il).

אביאת בר  
מהנדסת אבטחת מידע



## תקן ישראלי לאבטחת מידע ת"י 7799

מאת: מירב ורד, מנהלת תחום מתודולוגיה בחברת סקיריטרי.

מוסמכת ארגון BSI כ - BS7799 Lead Auditor

תקן 7799 הפך לסטנדרט בינלאומי המגדיר, מאפיין ומסמך ארגונים ברחבי העולם לקיום מערכת מתועדת לניהול אבטחת מידע. לפי אמות מידע מושכלות המותאמות למבנה הארגון, סיכוני האבטחתיים ועדיו העסקיים. התקן אומץ על-ידי מכון התקנים הישראלי, והוא הגוף המסמך היום בארץ לעמידה בתקן זה.

בדומה לתקן ISO 9000 המקובל בעולם כולו כרף אחיד בתחום האיכות, מתפתח תקן 7799 ותופס תאוצה ותפוצה בקרב גופים עסקיים רבים, הצפויים לבקש מספקיהם לעמוד בדרישות התקן אף הם. במערך כולל של ממשקים עסקיים הפועלים בקנה אחד עם דרישות התקן, ימוזערו נזקי המידע בארגון עצמו, ויצומצמו הפגיעות הפוטנציאליות בהיבט השיווקי והכספי. יכולת הארגון לתת מענה אבטחתי נאות לנתוני לקוחות הרגישים מחמת צנעת הפרט תתעצם, תמזער תביעות משפטיות מצד לקוחות ופגיעה בתדמית החברה.

התקן עוסק בכלל היבטי אבטחת המידע בארגון, במעגל האבטחה הפיזי, הלוגי ובמהימנות עובדים, הן מתוככי הארגון והן מחוצה לו. התקן מורכב משני חלקים, כאשר החלק השני מכיל את הפרמטרים המחייבים לעמידה בתקן ("דרישות למערכות ניהול אבטחת מידע"), ואילו החלק הראשון מפרט בהרחבה גדולה יותר את סעיפי החלק השני ומספק קווים מנחים ("קובץ כללים לניהול אבטחת מידע"). למעשה, אין התקן בא להכתיב לארגון את כלי ושיטות האבטחה, אלא נותן בידי מנהליו את שיקול הדעת בבחירת מדיניות אבטחת מידע שתשתלב עם הערכת



הסיכונים, המוגדרים בהתאם לאיומים על הנכסים, לנקודות התורפה, להשפעותיהן על הארגון ולדרגות הסיכון.

על הארגון לממש כלי ושיטות אבטחה העונים על 127 הבקורות המופיעות בתקן, או לחליפין, לספק הסבר נאות לביטול הצורך במימוש בקרה מסוימת.

מלבד התועלת הישירה שתניב חברה שתעמוד בדרישות התקן, משום הפיכתה לארגון מאובטח יותר שאפשרות התהוות סיכוני האבטחתיים תפחת, תהפוך החברה לגוף מוביל בארץ, העומד בסטנדרטים בינלאומיים בתחום אבטחת המידע ואשר עשוי להוות "סמן ימני" לחברות בארץ.