



שאלון הערכה עצמית A

הערה: השאלות הבאות ממוספרות בהתאם לנהלי הבדיקה ולדרישות PCI DSS כפי שהוגדרו במסמך דרישות ונהלי הערכת אבטחה של PCI DSS.
תאריך מילוי הטופס:

הטמע אמצעי בקרת גישה חזקים

דרישה 9: הגבל את הגישה הפיזית לנתונים של כרטיסי אשראי

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
9.5 האם כל סוגי המדיה, מאובטחים פיזית (לרבות, אך לא רק, מחשבים, אמצעי אחסון אלקטרוניים ניידים, קבלות נייר, דוחות נייר ופקסים)? למטרות דרישה 9, המונח "מדיה" מתייחס לכל הניירת ואמצעי האחסון האלקטרוניים המכילים נתוני כרטיסי האשראי.	- עבור על מדיניות והליכים לאבטחה פיזית של מדיה - ראיין את כוח האדם	☒	☐	☐	☐	☐
9.6 א. האם קיימת בקרה מחמירה על התפוצה הפנימית והחיצונית של כל סוגי המדיה?	- עבור על מדיניות והליכים לסיווג מדיה - ראיין עובדי אבטחה	☒	☐	☐	☐	☐
ב. האם הבקורות כוללות את הדברים הבאים:						
9.6.1 האם המדיות מסווגות כך שניתן לזהות מהי רמת הרגישות של המידע (המצוי בהן)?	- ראיין את כוח האדם - בחן את יומני הפצת המדיה והתיעוד	☒	☐	☐	☐	☐
9.6.2 האם המדיות נשלחות באמצעות שליח מאובטח או בשיטת מסירה אחרת המאפשרת לעקוב אחריהן באופן מדויק?	- ראיין את כוח האדם - בחן את	☒	☐	☐	☐	☐



שאלה					בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)
כן	כן עם CCW	לא	לא רלוונטי	לא נבדק		
					יומני הפצת המדיה והתיעוד	
☒	☐	☐	☐	☐	- האם נדרש אישור הנהלה לפני העברה של מדיות (במיוחד כשהן מופצות ליחידים)? - ראיין את כוח האדם - בחן את יומני הפצת המדיה והתיעוד	9.6.3
☒	☐	☐	☐	☐	- האם ישנה בקרה מחמירה על אופן האחסון והנגישות למדיות (המכילות נתוני כרטיסי אשראי)? - עבור על מדיניות והליכים	9.7
☒	☐	☐	☐	☐	- האם כל המדיות המכילות נתוני כרטיסי אשראי מושמדות כאשר אין בהן עוד צורך עסקי או חוקי? - עבור על מדיניות והליכים להשמדת מדיה תקופתית	9.8
					ג. האם המדיה מושמדת בצורה הבאה:	
☒	☐	☐	☐	☐	- האם מדיה קשיחה נגרסת, נשרפת או נכתשת באופן שאינו מאפשר לשחזר את הנתונים של כרטיסי האשראי? - ראיין את כוח האדם - בחן הליכים - צפה בהליכים	9.8.1
☒	☐	☐	☐	☐	- האם מכלים המאחסנים מידע המיועד להשמדה מאובטחים באופן המונע גישה לתכולתם? - בחן אבטחה של המכלים המאחסנים מידע	



יישם ותחזק מדיניות אבטחת מידע

דרישה 12: יישם ותחזק מדיניות הנותנת מענה לאבטחת מידע בקרב כלל כח האדם (עובדים וקבלנים)

הערה: לצרכי כוונת סעיף 12, "כח האדם" מתייחס לעובדים במשרה מלאה, עובדים במשרה חלקית, עובדים זמניים, קבלנים ויועצים שעובדים פיזית בתוך מתחמי הארגון או לחילופין שיש להם גישה לסביבת נתוני כרטיסי האשראי של החברה.

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
12.8 אם נתוני כרטיסי האשראי מועברים לספקי שירות אחרים, האם קיימים ומוטמעים מדיניות ונהלים לניהול ספקי השירות, כדלהלן?		☐	☐	☐	☐	☐
12.8.1 האם ישנה רשימה מתוחזקת של ספקי השירות?	- עבור על מדיניות והליכים - צפה בהליכים - עבור על רשימת ספקי השירות	☒	☐	☐	☐	☐
12.8.2 האם קיים הסכם בכתב הכולל הכרה באחריותו של ספק השירות לאבטחת נתוני כרטיסי האשראי הנמצאים ברשותו או שהוא מאחסן, מעבד או משדר עבור הלקוח, או במידה שהם יכולים להשפיע על האבטחה של סביבת נתוני כרטיסי האשראי של הלקוח? הערה: המינוח המדויק של ההכרה יהיה תלוי בהסכם בין שני הצדדים, פרטי השירות המסופק, והאחריות המוטלת על כל אחד מהצדדים. ההכרה לא חייבת לכלול את המינוח המדויק המופיע בדרישה זו.	- צפה בהסכמים הכתובים - עבור על מדיניות והליכים	☒	☐	☐	☐	☐
12.8.3 האם קיים תהליך מסודר להתחלת העסקה של ספק	צפה בתהליכים	☒	☐	☐	☐	☐



שאלה					בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)
כן	כן עם CCW	לא	לא רלוונטי	לא נבדק		
					עבור על מדיניות והליכים ומסמכים ותומכים	
☒	☐	☐	☐	☐	- צפה בתהליכים - עבור על מדיניות והליכים ומסמכים ותומכים	12.8.4 האם קיימת תכנית כדי לנטר אחר מצב התאימות של ספקי השירות לתקן PCI DSS לפחות פעם בשנה?
☒	☐	☐	☐	☐	- צפה בתהליכים - עבור על מדיניות והליכים ומסמכים ותומכים	12.8.5 האם נשמר מידע בנוגע לאילו דרישות PCI DSS מטופלות על ידי איזה ספק שירות, ואילו מטופלות על ידי הארגון?