נציג בית העסק הנכבד,

מסמך זה הינו תרגום שאלון ההערכה העצמית SAQ. המסמך תורגם מהשפה האנגלית לשפה העברית על מנת לסייע לך במילוי הדרישות.

יודגש כי המסמך המקורי נכתב בשפה האנגלית והוא הנוסח המחייב.

התרגום העברי פונה לנשים וגברים כאחד ונוסח בלשון זכר מטעמי נוחות בלבד.

למרות כל המאמצים והזהירות בתרגום הדרישות מהשפה האנגלית, חברת EverCompliant ו/או חברות האשראי ; ישראכרט בע"מ, לאומי קארד בע"מ וכ.א.ל בע"מ (להלן: "הארגונים") אינם ערבות לטיב התרגום ו/או דיוקו.

לכן הארגונים לא יישאו בכל אחריות ו/או נזק עקב השימוש במסמך בשפה העברית.

מודגש בזאת כי הנעזר במסמך המתורגם בשפה העברית לצורך מילוי השאלון המקורי עושה זאת על דעתו ועל אחריותו בלבד.

בברכה,

ישראכרט

תעשיית כרטיסי התשלום (PCI)
תקן אבטחת מידע
שאלון הערכה עצמית B (SAQ)
והצהרת תאימות

בתי עסק עם מכונות סליקה ידנית או מסופים עצמאיים בעלי יציאה ייעודית, אין שמירה אלקטרונית של נתוני אשראי

גרסה 3.0

פברואר 2014

שינויי מסמך

תאריך	גרסה	תיאור
אוקטובר 2008	1.2	התאמת התוכן לתקן PCI DSS החדש גרסה 1.2 והכנסת שינויים משניים שחלו מאז גרסה 1.1 המקורית
אוקטובר 2010	2.0	התאמת התוכן לדרישות ולנהלי הבדיקה של תקן PCI DSS החדש גרסה 2.0
פברואר 2014	3.0	התאמת התוכן לדרישות ולנהלי הבדיקה של תקן PCI DSS החדש גרסה 3.0 ולשלב אפשרויות תגובה נוספות.

תוכן עניינים

לפני שמתחילים

שאלון הערכה עצמית B פותח עבור בתי עסק רלוונטיים המעבדים נתוני אשראי אך ורק באמצעות סליקה ידנית או באמצעות מסופים עצמאיים בעלי יציאה ייעודית בלבד.

בתי עסק המתאימים למילוי שאלון B עשויים להיות בתי עסק המבצעים עסקאות פנים מול פנים (כרטיס נוכח), מסחר אלקטרוני או הזמנות בטלפון/דואר (עסקאות ללא כרטיס נוכח). ואינם מאחסנים נתוני כרטיס אשראי בשום סביבה ממוחשבת.

בתי עסק אלו מאשרים את עמידתם בתקן באמצעות מילוי שאלון B, המאמתים כי:

- הארגון משתמש אך ורק בסליקה ידנית או במסופים עצמאיים בעלי יציאה ייעודית (באמצעות קו טלפון לספק המעבד את נתוני האשראי) לצורך קבלת נתוני האשראי מהלקוחות;
- המסופים העצמאיים בעלי היציאה הייעודית, אינם מחוברים לשום מערכת נוספת בתוך הארגון;
- המסופים העצמאיים בעלי יציאה ייעודית, אינם מחוברים לאינטרנט;
- הארגון אינו מעביר נתוני כרטיס אשראי דרך הרשת (ברשת פנימית או האינטרנט).
- הארגון שומר רק דוחות נייר או העתקי נייר של קבלות עם נתוני אשראי, ומסמכים אלו אינם מתקבלים בצורה אלקטרונית; בנוסף
- הארגון אינו שומר נתוני אשראי בפורמט אלקטרוני.

אפשרות זו אינה חלה בשום פנים ואופן על בתי עסק המקיימים מסחר עם עמדות מכירה "פנים מול פנים".

כל חלק בשאלון מתמקד בתחום ספציפי של אבטחת המידע, תוך התבססות על הדרישות המפורטות בתקן *PCI DSS*. גרסה מקוצרת זו של שאלון הערכה עצמית כוללת שאלות הרלוונטיות לסוג מסוים של בתי עסק קטנים, כמוגדר לעיל. במידה ויש דרישות בתקן אשר רלוונטיות לסביבה הארגונית שלך ואינן נמצאות בשאלון זה, אזי ככל הנראה שאלון זה אינו מתאים לארגון שלך. בנוסף לכך, על הארגון שלך לעמוד בכל הדרישות הרלוונטיות של התקן, על מנת להיות תואם לתקן.

הערכה עצמית PCI DSS – שלבי ביצוע

1. יש לזהות את שאלון ההערכה העצמית המתאים לסביבת המסחר הספציפית – למידע, עיין במסמך *Self-Assessment Questionnaire Instructions and Guidelines* באתר האינטרנט של PCI SSC.
2. יש לוודא שסביבת המסחר הוערכה כראוי והיא נכללת בקריטריונים של השאלון שבו נעשה שימוש.
3. יש לבצע הערכה של תאימות סביבת העבודה לדרישות PCI DSS.
4. יש למלא את כל החלקים של מסמך זה:
   - פרק 1 (פרק 1 ו-2 של AOC) – פרטי הערכה ותקציר מנהלים.
   - פרק 2 – שאלון הערכה עצמית של PCI DSS (שאלון הערכה עצמית D)
   - פרק 3 (חלקים 3 ו-4 של AOC) – אשרור פרטי הצהרת התאימות ותוכנית פעולה לסטטוס 'לא עומד בתקן' (במידה ורלוונטי)
5. יש להגיש את שאלון ההערכה העצמית ואת הצהרת התאימות, בצירוף כל מסמך נדרש אחר – כגון דוחות סריקה מאת ספק הסריקות המאושר – לחברת כרטיסי האשראי, לחברה המחזיקה במותג האשראי או לכל דורש אחר.

הבנת שאלון ההערכה העצמית

השאלות המופיעות תחת העמודה "שאלה" בשאלון הערכה עצמית זה מבוססות על דרישות תקן PCI DSS.

משאבים נוספים המספקים הנחיה לדרישות PCI DSS ואופן המילוי של שאלון ההערכה העצמית מצורפים על מנת לסייע לך בתהליך ההערכה. להלן סקירה של חלק ממסמכים אלה:

מסמך	כולל:
PCI DSS *(תקן PCI לאבטחת מידע:* *דרישות ונהלי הערכת אבטחה)*	• הנחיות לגבי היקף הסקירה • הנחיות לגבי כוונת דרישות PCI DSS • פרטים על נהלי הבדיקה • הנחיות לגבי בקרות מפצות
מסמכי הוראות והנחיות להערכה עצמית	• מידע על כל שאלוני ההערכה העצמית והקריטריונים להכללה • כיצד לקבוע איזה שאלון הערכה מתאים לעסק/לארגון שלך
תקן PCI לאבטחת מידע ותקן אבטחת נתונים של יישומי תשלום: *מילון מונחים, קיצורים וראשי תיבות*	• תיאורים והגדרות של המונחים שבהם נעשה שימוש בתקן PCI DSS ובשאלוני ההערכה העצמית

משאבים אלה ואחרים מופיעים באתר האינטרנט של מועצת תקני האבטחה הרשמית של PCI (PCI SSC) בכתובת www.pcisecuritystandards.org. ארגונים מתבקשים לעבור על מסמכי PCI DSS ועל מסמכי התמיכה האחרים לפני ביצוע ההערכה.

בדיקות נדרשות

ההוראות המופיעות תחת העמודה "בדיקות נדרשות" מבוססות על נהלי הבדיקה של תקן PCI DSS, ומספקות תיאור מפורט של סוגי פעילויות הבדיקה שיש לערוך על מנת לוודא שהדרישה אכן נענתה. פרטים מלאים על נהלי הבדיקה עבור כל דרישה ניתן למצוא ב-PCI DSS.

מילוי שאלון ההערכה העצמית

בכל שאלה קיימת בחירה בין מספר תגובות המציינות את מצב החברה בנוגע לאותה דרישה. ***יש לבחור תגובה אחת בלבד לכל שאלה.***

בטבלה להלן תיאור של כל תגובה:

תגובה	מתי יש להשתמש בתגובה זו:
כן	הבדיקות הנדרשות בוצעו וכל מרכיבי הדרישה נענו כפי שהוצהר.
כן עם גיליון עבודה של בקרות מפצות	הבדיקות הנדרשות בוצעו והדרישה נענתה בסיוע בקרה מפצה. כל התגובות בעמודה זו מחייבות מילוי גיליון בקרות מפצות (CCW) המופיע בנספח ב' של שאלון ההערכה העצמית. מידע על השימוש בבקרות מפצות והנחיות למילוי גיליון העבודה מופיעים ב-PCI DSS.
לא	חלק ממרכיבי הדרישה או כולם לא נענו, או נמצאים בתהליך של הטמעה ויישום, או שנדרשות בדיקות נוספות לקבלת מידע על קיומן של דרישות אלה.
לא רלוונטי	הדרישה אינה חלה על הסביבה הארגונית הספציפית (ר' *הנחיה בנוגע לחוסר הרלוונטיות של דרישות ספציפיות* מסוימות להלן). כל התגובות בעמודה זו מחייבות הסבר תומך בנספח ג' של שאלון ההערכה העצמית.
לא נבדק	הדרישה לא עמדה לשיקול בהערכה ולא נבדקה בדרך כלשהי (לדוגמאות לגבי השימוש באפשרות זו, ר' *הבנת ההבדל בין האפשרות 'לא רלוונטי' לאפשרות 'לא נבחן'*).

	כל התגובות בעמודה זו מחייבות הסבר תומך בנספח ג' של שאלון ההערכה העצמית.

הנחיה בנוגע לחוסר הרלוונטיות של דרישות ספציפיות מסוימות

אם דרישות כלשהן אינן רלוונטיות לסביבת האשראי של החברה יש לבחור באפשרות "לא רלוונטי" עבור אותה דרישה מסוימת, ולמלא את גיליון "הסבר לחוסר רלוונטיות" שבנספח ג' עבור כל בחירה כגון זו.

החרגה משפטית

אם הארגון נתון להגבלה משפטית המונעת ממנו לעמוד בדרישות מסוימות של תקן PCI DSS, יש לסמן את העמודה "לא" עבור דרישות אלה ולמלא את ההצהרה הרלוונטית בחלק 3.

פרק 1 – פרטי ההערכה

הוראות הגשה

על בית העסק למלא מסמך זה כהצהרה על תוצאות ההערכה העצמית של בית העסק ל*'דרישות ונהלי האבטחה של תקן אבטחת המידע של תעשיית כרטיסי האשראי'* (PCI DSS). השלם את כל החלקים: על בית העסק להבטיח את מילוי כל אחד מהחלקים של שאלון זה על-ידי הצדדים הרלוונטיים. בכל הנוגע לנהלי הדיווח וההגשה של המסמך, יש ליצור קשר עם חברת כרטיסי האשראי (בנק מסחרי) או עם החברה המחזיקה במותג האשראי.

חלק 1. פרטי בית העסק וחברת ההסמכה הרשמית (QSA) **חלק 1א. פרטי בית העסק**			
שם החברה:		שם(ות) מסחרי(ים):	
שם איש קשר:		תפקיד:	
שם גורם ההסמכה הפנימי (אם רלוונטי):		תפקיד:	
טלפון:		דוא"ל:	
כתובת העסק:		עיר:	
מדינה:		מיקוד:	
אתר אינטרנט:			

חלק 1ב. פרטי חברת ההסמכה הרשמית (QSA- אם רלוונטי)			
שם החברה:			
שם הסוקר המוסמך הראשי:		תפקיד:	
טלפון:		דוא"ל:	
כתובת העסק:		עיר:	
מדינה:		מיקוד:	
אתר אינטרנט:			

חלק 2. תקציר מנהלים

חלק 2א. סוג העסק המסחרי (יש לסמן את כל הרלוונטיים)

☐ קמעונאי ☐ טלקומוניקציה ☐ מרכולים וסופרמרקטים

☐ דלק ☐ מסחר אלקטרוני ☐ הזמנות דואר/טלפון

☐ אחר (אנא פרט):

אלו סוגים של ערוצי תשלום מציע בית העסק?	אלו ערוצי תשלום כלולים בשאלון הערכה עצמית זה?
☐ הזמנות דואר/טלפון	☐ הזמנות דואר/טלפון
☐ מסחר אלקטרוני	☐ מסחר אלקטרוני
☐ נוכחות כרטיס (פנים אל פנים)	☐ נוכחות כרטיס (פנים אל פנים)

הערה: *אם הארגון מציע תהליכים או ערוצי תשלום שאינם נכללים בשאלון הערכה עצמית זה, יש להיוועץ בחברת כרטיסי האשראי או במותג האשראי בנוגע לאשרור ערוצי התשלום האחרים.*

חלק 2ב: תיאור סביבת כרטיסי האשראי

באיזה אופן ועד כמה בית העסק מעבד, מאחסן או משדר פרטי כרטיסי אשראי?	

חלק 2ג: מיקומים

פרט את סוגי המתקנים והאתרים הנכללים בסקר ה-PCI DSS (לדוגמה, חנויות מסחריות, משרדים ארגוניים, מרכזי נתונים, מוקדים טלפוניים וכיו"ב)

סוג המתקן	מיקום(י) המתקן (עיר, מדינה)

חלק 2ד: מערכות תשלום

האם הארגון משתמש במערכת תשלום אחת או יותר? ☐ כן ☐ לא

ספק את המידע הבא בנוגע למערכות התשלום שבהם נעשה שימוש בארגונך:

שם מערכת התשלום	מספר גרסה	יצרן מערכת התשלום	האם מערכת התשלום מאושרת לתקן PA-DSS?	תאריך תפוגה של אישור PA-DSS (אם רלוונטי)
			☐ כן ☐ לא	
			☐ כן ☐ לא	
			☐ כן ☐ לא	

חלק 2ה: תיאור הסביבה

הצג תיאור ***<u>פרטני</u>*** של הסביבה הנכללת בהערכה זו. *לדוגמה:* • *חיבורים לתוך סביבת נתוני האשראי (CDE) וממנה.* • *רכיבי מערכת קריטיים בתוך סביבת נתוני האשראי, כגון מסופי נקודות מכירה (POS), בסיסי נתונים, שרתי אינטרנט וכיו"ב, וכן כל רכיבי תשלום חיוניים אחרים.*	
האם נעשה שימוש בסגמנטציית רשת המשפיעה על היקפה של סביבת ה-PCI DSS? (עיין בחלק "סגמנטציית רשת" של PCI DSS להנחיות בנוגע לסגמנטציה של הרשת הארגונית)	☐ כן ☐ לא

חלק 2ו: שירותי צד ג'

האם החברה משתפת את נתוני כרטיסי האשראי עם ספקים של שירותי צד ג' (לדוגמה, שירותי גישה לרשת, שירותי עיבוד תשלומים, ספקים של שירותי תשלום (PSP), חברות אירוח אתרים, סוכני הזמנת טיסות, סוכני תוכניות נאמנות וכיו"ב)?	☐ כן ☐ לא

אם כן:

שם ספק השירות:	תיאור השירות הניתן:

הערה: *דרישה 12.8 חלה על כל הישויות ברשימה זו.*

חלק 2ז: סיווג מתאים למילוי שאלון B	
בית העסק מאשר כי סיווגו מתאים למילוי גרסה מקוצרת זו של שאלון הערכה עצמית מהנימוקים הבאים:	
☐	בית העסק משתמש אך ורק במכונות סליקה ידנית כדי להדפיס נתוני אשראי של הלקוחות ולא משדר נתוני אשראי על גבי קו טלפון או אינטרנט; או בית העסק משתמש אך ורק במסופים עצמאיים בעלי יציאה ייעודית, אשר אינם מחוברים לאינטרנט או לכל מערכת אחרת ברחבי הארגון;
☐	בית העסק אינו מעביר נתוני כרטיס אשראי דרך הרשת (הן ברשת פנימית והן באינטרנט)
☐	בית העסק אינו מאחסן כלל נתונים של כרטיסי אשראי בפורמט אלקטרוני; **ובנוסף**
☐	אם בית העסק מחזיק בכל זאת נתוני כרטיסי אשראי, מידע זה מופיע אך ורק על דוחות וקבלות נייר ואינו מתקבל בצורה אלקטרונית.

פרק 2 : שאלון הערכה עצמית B

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

תאריך מילוי הטופס:

הגנה על נתוני אשראי

דרישה 3: הגן על הנתונים המאוחסנים של כרטיסי האשראי

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
3.2	ד. האם מידע אימות רגיש מושמד או אינו ניתן לשחזור לאחר השלמת הליך האימות?	• עבור על המדיניות וההליכים • בחן את הקונפיגורציה של המערכת • בחן את דרישות השמירה	☐	☐	☐	☐	☐
	ה. האם כל המערכות עונות לדרישות הבאות בנוגע לאי-שמירה של מידע אימות רגיש לאחר אישור עסקה (אפילו אם הוא מוצפן)?						
3.2.1	האם תכולתו המלאה של אף אחד מהערוצים (track) מהפס המגנטי (הממוקם בגב הכרטיס, או מידע זהה הממוקם על שבב או בכל מקום אחר) אינה נשמרת לאחר אימות? *מידע זה גם נקרא ערוץ מלא (full track), ערוץ 1 (track 1), ערוץ 2 (track 2) ופרטי הפס המגנטי.* *הערה: ייתכן ובמהלכם הרגיל של העסקים יהיה צורך לשמור את הפרטים הבאים המצויים בפס המגנטי:* ▪ *שם בעל הכרטיס* ▪ *מספר כרטיס האשראי (PAN)* ▪ *תאריך התפוגה (תוקף)* ▪ *וקוד השירות*	• בחן מקורות מידע כולל: • מידע נכנס על עסקאות • כל הרשומות • קבצי היסטוריה • קבצי ערוצים • סכמת מאגר המידע • תוכן מאגר המידע	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	על מנת לצמצם את הסיכון, שמור רק את הפרטים הללו כאשר יש צורך עסקי בכך.						
3.2.2	האם הקוד (CVC) או ערך הקוד (CVV) לאימות הכרטיס (המספר בעל שלוש או ארבע ספרות המודפס בקדמת או בגב הכרטיס) אינו נשמר לאחר האימות?	• בחן מקורות מידע כולל: • מידע נכנס על עסקאות • כל הרשומות • קבצי היסטוריה • קבצי ערוצים • סכמת מאגר המידע • תוכן מאגר המידע	☐	☐	☐	☐	☐
3.2.3	האם מספר הזיהוי האישי (PIN) או בלוק מידע הכולל את ה PIN המוצפן אינם נשמרים לאחר האימות?	• בחן מקורות מידע כולל: • מידע נכנס על עסקאות • כל הרשומות • קבצי היסטוריה • קבצי ערוצים • סכמת מאגר המידע • תוכן מאגר המידע	☐	☐	☐	☐	☐
3.3	האם מספר כרטיס האשראי ממוסך כאשר הוא מוצג (שש הספרות הראשונות וארבע הספרות האחרונות הן המספר המקסימלי של ספרות שיוצגו) כך שרק עובדים עם צורך עסקי לגיטימי יוכלו לראות את ה-PAN המלא? *הערה: דרישה זו אינה גוברת על דרישות מחמירות יותר הנוגעות*	• עבור על המדיניות והנהלים • עבור על התפקידים שצריכים גישה לתצוגה מלאה של ה-PAN • בחן את קונפיגורציית	☐	☐	☐	☐	☐

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
להצגה של נתוני מחזיקי כרטיסי אשראי – למשל דרישות סוג כרטיס תשלום או דרישות משפטיות בנוגע לקבלות בנקודות מכירה (POS)	המערכת • צפה בתצוגות של PAN					

דרישה 4: הצפן את השידור של נתוני כרטיסי אשראי על פני רשתות ציבוריות פתוחות

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
4.2	ב. האם ישנם נהלים הקובעים כי אין לשלוח מספרי כרטיסי אשראי בלתי מוגנים באמצעות טכנולוגיות העברת מסרים של משתמשי קצה?	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐

הטמע אמצעי בקרת גישה חזקים

דרישה 7: הגבל את הגישה לפרטי כרטיסי האשראי עפ"י העקרון של הצורך העסקי לדעת

שאלה		דרישות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
7.1	האם הגישה לרכיבי מערכת ולנתוני כרטיסי אשראי מוגבלת רק לאנשים שתפקידם מחייב זאת, כדלקמן:						
7.1.2	האם הקצאת ההרשאות המיוחדות לעובדים המורשים מוגבלת כדלקמן? • למספר ההרשאות המינימלי הדרוש למילוי התפקיד? • הקצאה רק לתפקידים שדורשים גישה מסווגת זו?	• ראיין את כוח האדם • ראיין את ההנהלה • עבור על מספרי משתמש מסווגים	☐	☐	☐	☐	☐
7.1.3	האם גישה מאושרת בהתבסס על הסיווג והתפקוד של כל תפקיד?	• ראיין את ההנהלה • עבור על מספרי המשתמש	☐	☐	☐	☐	☐

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 הבקרות 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 יומני הפצת המדיה והתיעוד	☐	☐	☐	☐	☐
9.6.3	האם נדרש אישור הנהלה לפני העברה של מדיות (במיוחד כשהן מופצות ליחידים)?	• ראיין את כוח האדם • בחן את יומני הפצת המדיה והתיעוד	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
9.7	האם ישנה בקרה מחמירה על אופן האחסון והנגישות למדיות (המכילות נתוני כרטיסי אשראי)?	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
9.8	א. האם כל המדיות המכילות נתוני כרטיסי אשראי מושמדות כאשר אין בהן עוד צורך עסקי או חוקי?	• עבור על מדיניות והליכים להשמדת מדיה תקופתית	☐	☐	☐	☐	☐
	ג. האם המדיה מושמדת בצורה הבאה:						
9.8.1	א. האם מדיה קשיחה נגרסת, נשרפת או נכתשת באופן שאינו מאפשר לשחזר את הנתונים של כרטיסי האשראי? ?	• ראיין את כוח האדם • בחן הליכים • צפה בהליכים	☐	☐	☐	☐	☐
	ב. האם מכלים המאחסנים מידע המיועד להשמדה מאובטחיםבאופן המונע גישה לתכולתם?	• בחן אבטחה של המכלים המאחסנים מידע	☐	☐	☐	☐	☐
9.9	האם מכשירים המאחסנים נתוני כרטיסי אשראי דרך ממשק פיזי עם הכרטיס מוגנים נגד החלפה והתעסקות ? ***הערה:*** *דרישה זו מתייחסת למכשירי קריאת כרטיסים המשמשים בעסקאות בהם הכרטיס נוכח פיזית (יש העברת כרטיס פיזית) בנקודת המכירה. דרישהזו לא מתייחסת לרכיבים של הקלדה ידנית כגון על מקלדות מחשבים או POS.* ***הערה:*** *דרישה 9.9 מהווה המלצה עד ל-30 ביוני, 2015,*						

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
ולאחר מכן תהפוך לדרישה.							
	א. האם המדיניות וההליכים מחייבים שמירת רשימה של מכשירים כאלו?	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
	ב. האם המדיניות וההליכים מחייבים בדיקה תקופתית של מכשירים אלו לגילוי התערבות או החלפה?	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
	ג. האם המדיניות וההליכים מחייבים הכשרה של העובדים לעירנות להתנהגות חשודה ולדיווח התערבות או החלפה של המכשירים?	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
9.9.1	א. האם רשימת המכשירים כוללת את הנתונים הבאים? • סוג, מודל המכשיר. • מיקום המכשיר (לדוגמה, כתובת האתר או המתקן בו נמצא המכשיר) • מספר סידרתי של המכשיר או שיטת זיהוי ייחודית אחרת	• בחן את רשימת המכשירים	☐	☐	☐	☐	☐
	ב. האם הרשימה מדויקת ומעודכנת?	• צפה במיקום המכשירים והשווה לרשימה	☐	☐	☐	☐	☐
	ג. האם רשימת המכשירים מעודכנת כאשר מכשירים מתווספים, משנים	• ראיין את כוח האדם	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	מיקום, יוצאים מכלל פעולה, ועוד?						
9.9.2	א. האם משטחי המכשירים נבדקים תקופתית כדי לגלות התערבות (לדוגמה, הוספה של קוראי כרטיסים למכשיר) או החלפה (לדוגמה, על ידי בדיקת המספר הסידרתי או מאפייני מכשיר אחרים לוודא שהמכשיר לא הוחלף בזיוף) כדלקמן: ***הערה:*** *דוגמאות לסימנים של התעסקות או החלפה של מכשיר כוללים תוספות לא צפויות או כבלים המחוברים למכשיר, תוויות אבטחה חסרות או שונות, כיסוי שבור או בצבע שונה, או שינויים במספר הסידרתי או סימנים חיצוניים אחרים.*	• ראיין את כוח האדם • צפה בהליכי הבדיקה והשווה להליכים המוגדרים	☐	☐	☐	☐	☐
	ב. האם העובדים מודעים להליכים לבדיקת המכשירים?	• ראיין את כוח האדם	☐	☐	☐	☐	☐
9.9.3	האם העובדים מקבלים הכשרה כדי להיות ערנים לאפשרות של מכשירים שהוחלפו או התעסקו איתם, כולל הבאים:						
א.	• האם חומרי ההכשרה עבור עובדים בנקודות מכירה כוללים את הנקודות הבאות? • אימות זיהוי של אנשים מצד שלישי הטוענים שהם עובדי תחזוקה או שירות לפני שהם מקבלים גישה	• עבור על חומר ההכשרה	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	• לשנות או לתקן מכשירים • אין להתקין, להחליף, או להשיב מכשירים ללא אימות • יש לשים לב להתנהגות חשודה סביב מכשירים (לדוגמה, ניסיונות של אנשים לא ידועים לפתוח מכשירים או לנתקם) • יש לדווח לעובדים המתאימים (כגון מנהל או קצין אבטחה) על התנהגות חשודה וסימנים של התעסקות או החלפה של המכשיר.						
ב.	• האם העובדים בנקודות המכירה קיבלו הכשרה, והם מודעים להליכים לגילוי ודיווח ניסיונות להתעסק עם המכשירים או להחליפם?	• ראיין עובדים בנקודות המכירה	☐	☐	☐	☐	☐

יישם ותחזק מדיניות אבטחת 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
12.1	האם מדיניות האבטחה קיימת, מפורסמת, מתוחזקת ומופצת לכל כח האדם הרלוונטי?	▪ עבור על מדיניות אבטחת המידע	☐	☐	☐	☐	☐
12.1.1	האם מדיניות אבטחת המידע נסקרת/נבדקת לפחות אחת לשנה ומעודכנת בהתאם לצורך על מנת לשקף שינויים ביעדי העסק ובסביבת הסיכונים שלו?	▪ עבור על מדיניות אבטחת המידע ▪ ראיין עובדים אחראיים	☐	☐	☐	☐	☐
12.3	האם פותחה מדיניות שימוש בטכנולוגיות קריטיות על מנת להבטיח את השימוש הנאות בטכנולוגיות הללו ואשר כוללת את הדרישות הבאות: ***הערה:*** *טכנולוגיות קריטיות כוללות לדוגמה, אבל לא רק, טכנולוגיות גישה מרחוק, טכנולוגיות אלחוטיות, מדיות אלקטרוניות נשלפות, מחשבים ניידים, טבלטים, מחשבי כף יד, דוא"ל ואינטרנט*						
12.3.1	אישור מפורש מטעם גורמים מורשים לשימוש בטכנולוגיות?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.3	רשימה של המכשירים מסוג זה	▪ עקוב אחר	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	והעובדים בעלי הגישה?	מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים					
12.3.5	שימושים מקובלים בטכנולוגיה?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
	א. האם המדיניות מכילה דרישה עבור אנשים עם הרשאה מתאימה להגן על נתוני כרטיסי האשראי בהתאם לדרישות תקן PCI DSS?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.4	האם המדיניות ונהלי האבטחה מגדירים בבירור את תחומי האחריות של כל עובד בכל הקשור לאבטחת מידע?	▪ עבור על מדיניות והליכים של אבטחת מידע ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.5	ב. האם סמכויות הניהול הבאות בתחום אבטחת המידע מוקצות לאדם או לקבוצה:						
12.5.3	פיתוח, תיעוד והפצת נהלי תגובה לאירועי אבטחה ותהליכי הסלמה (אסקלציה) על מנת להבטיח טיפול יעיל ומתוזמן היטב בכל מצבי האבטחה?	▪ עבור על מדיניות והליכים של אבטחת מידע	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
12.6	א. האם ישנה תכנית מודעות אבטחה רשמית שתפקידה לגרום לכלל העובדים להיות מודעים לחשיבות אבטחת נתוני כרטיסי אשראי?	▪ עבור על התוכנית למודעות לאבטחה	☐	☐	☐	☐	☐
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 שירות, לרבות בדיקת נאותות הולמת לפני תחילת העבודה מולו?	▪ צפה בתהליכים ▪ עבור על מדיניות והליכים	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		ומסמכים תומכים					
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 תומכים	☐	☐	☐	☐	☐
12.8.5	האם נשמר מידע בנוגע לאילו דרישות PCI DSS מטופלות על ידי איזה ספק שירות, ואילו מטופלות על ידי הארגון?	▪ צפה בתהליכים ▪ עבור על מדיניות והליכים ומסמכים תומכים	☐	☐	☐	☐	☐
12.10.1	א. האם פותחה תכנית תגובה לאירוע אבטחה שניתן ליישמה במקרה של אירוע פריצת אבטחה במערכת?	▪ עבור על תוכנית תגובה לאירוע ▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐

נספח א': דרישות נוספות עבור ספקי אירוח משותף (Shared Hosting Providers)

נספח זה אינו לשימוש הערכת בתי עסק.

נספח ב': גיליון בקרות מפצות

יש להשתמש בגיליון עבודה זה כדי להגדיר את הבקרות המפצות עבור כל אחת מן הדרישות אשר סומנה עבורה התשובה " כן עם גליות עבודה של בקרות מפצות".

הערה: *רק חברות שביצעו הערכת סיכונים ושיש להן אילוצים עסקיים או טכנולוגיים מתועדים לגיטימיים רשאיות לעשות שימוש בבקרות מפצות על מנת לעמוד בתקן.*

עיין בנספחים B,C ו- D של מסמך PCI DSS לקבלת מידע על בקרות מפצות והדרכה כיצד להשלים גיליון זה.

מספר הדרישה והגדרתה:

	מידע נדרש	הסבר
1. אילוצים	מנה את האילוצים המונעים עמידה בדרישת התקן המקורית.	
2. יעד	הגדר את יעד הבקרה המקורית ; זהה את היעד המושג על ידי הבקרה המפצה.	
3. הסיכון המזוהה	זהה סיכונים נוספים הנובעים מהעדרו של אמצעי הבקרה המקורי.	
4. הגדרה הבקרה המפצה	הגדר את הבקרות המפצות והסבר כיצד הן נותנות מענה ליעדי הבקרה המקורית והסיכון המוגבר, אם קיים.	
5. בדיקת תקפות הבקרה המפצה	הגדר כיצד נבדקו הבקרות המפצות וכיצד אושררה תקפותן.	
6. תחזוקה	הגדר את התהליכים ואמצעי הבקרה המיושמים לצורך תחזוקת הבקרות המפצות.	

נספח ג': הסבר על חוסר רלוונטיות (N/A)

במידה והוזן ערך "N/A" או "לא רלוונטי", יש להשתמש בגיליון עבודה זה כדי להסביר מדוע הדרישה האמורה אינה רלוונטית לארגון.

דרישה	הסיבה לחוסר הרלוונטיות
דוגמה: *3.4*	*נתוני כרטיסי האשראי אף פעם לא מאוחסנים באופן אלקטרוני.*

חלק 3 – אישור ואימות פרטים

חלק 3. אישור PCI DSS

בהסתמך על התוצאות שהתקבלו בשאלון B מתאריך *(תאריך מילוי השאלון)*, *(שם נותן שירות)* מצהיר על סטטוס התאימות הבא (יש לסמן אחד):

☐ **עומד בתקן**: כל חלקי שאלון PCI SAQ מולאו וכל השאלות נענו בחיוב ולפיכך הדירוג הכללי של החברה הוא **עומד בתקן**, **ובנוסף** סריקה עם ציון עובר בוצעה על ידי ספק סריקות מאושר (ASV) בהתאם לכך *(שם נותן שירות)* הראה תאימות מלאה לדרישות PCI DSS.

☐ **לא עומד בתקן:** לא מולאו כל חלקי שאלון PCI SAQ, או שישנן שאלות שהתשובה אליהן היתה "לא", ולכן דירוגה הכללי של החברה **לא עומד בתקן**, **או** לא בוצעה סריקה עם ציון עובר על ידי ספק סריקות מאושר (ASV), לפיכך *(שם נותן שירות)* לא הראה תאימות מלאה לדרישות PCI DSS.

- **תאריך יעד** לתאימות לתקן:
- ישות עסקית המגישה טופס זה עם סטטוס 'לא עומד בתקן' עשויה להידרש לביצוע 'תוכנית הפעולה' המפורטת בחלק 4 שבמסמך זה. *יש לברר מול חברת כרטיסי האשראי או מותג(י) האשראי שאיתו(ם) אתם עובדים לפני ביצוע חלק 4 הואיל ולא כל חברות מותגי האשראי דורשות חלק זה.*

☐ **עומד בתקן אבל עם החרגה משפטית:** אחד או יותר מהדרישות סומנו "לא" בשל מגבלה משפטית המונעת מהדרישה להתקיים. אפשרות זו מחייבת בחינה נוספת של חברת האשראי. אם אופציה זו סומנה, השלם את הטבלה הבאה:

דרישה רלוונטית	פירוט כיצד מגבלה משפטית מונעת מהדרישה להתקיים

חלק 3א. אישור סטטוס התאימות

נותן השירות מאשר כי:

☐	שאלון הערכה עצמית B של PCI DSS, גרסה (מס' הגרסה של השאלון), הושלם בהתאם להוראות המופיעות בו.
☐	כל המידע הנכלל בשאלון האמור ובהצהרה זאת מייצג נאמנה את תוצאות ההערכה שלי בכל ההיבטים המהותיים.
☐	אישרתי עם ספק התשלומים שלי כי מערכת התשלומים אינה מאחסנת נתוני אימות רגישים לאחר קבלת אישור.
☐	קראתי את תקנות PCI DSS ואני מכיר בזאת כי מחובתי לשמור על תאימות מלאה ל-PCI DSS בכל זמן.
☐	אם הסביבה שלי משתנה, אני מכיר בך שאני חייב להעריך מחדש את הסביבה שלי וליישם את כל

	דרישות PCI DSS נוספות שחלות.
☐	לא נמצאו כל ראיות לשמירה של נתוני הפס המגנטי[1], נתוני CAV2, CVC2, CID, או CVV2 [2], או נתוני PIN [3], לאחר אישור עסקה **באף אחת** מהמערכות שנבדקו במהלך הערכה זו.
☐	סריקות ASV הושלמו ומתבצעות על ידי ספר סריקה PCI DSS מאושר (שם ספק סקירה).

חלק 3ב. אישור נותן השירות	
חתימה של מנהל בכיר בבית העסק ↑	*תאריך* ↑
שם המנהל הבכיר בבית העסק ↑	*תפקיד* ↑

חלק 3ג. אישור QSA (אם רלוונטי)	
אם QSA היה מעורב או סייע בהערכה זו, תאר את התפקיד שבוצע:	
חתימה של נציג QSA: ↑	*תאריך* ↑
שם נציג QSA:	*חברת QSA:*

חלק 3ד. אישור ISA (אם רלוונטי)	
אם ISA היה מעורב או סייע בהערכה זו, תאר את התפקיד שבוצע:	
חתימה של נציג ISA: ↑	*תאריך* ↑
שם נציג ISA:	*תפקיד:*

[1] נתונים המקודדים בפס המגנטי או מידע דומה על שבב המשמשים לאישור בעסקאות בהן הכרטיס נוכח. יישויות אינן רשאיות לשמור את נתוני הפס המגנטי במלואם לאחר אישור העסקה. הערכים היחידים המצויים על הפס המגנטי ומותרים לשמירה הינם מספר הכרטיס, תאריך תפוגה, ושם בעל הכרטיס.

[2] המספר בעל שלוש או ארבע הספרות המודפס על תיבת החתימה או מימין לתיבת החתימה או על חזית הכרטיס האשראי המשמש לביצוע אימות בעסקאות בהן הכרטיס אינו נוכח.

[3] הקוד הסודי האישי המוקלד על ידי בעל הכרטיס בעסקאות בהן הכרטיס נוכח, ו/או מספר PIN מוצפן בהודעת העסקה.

חלק 4. תוכנית פעולה לסטטוס 'לא עומד בתקן'

אנא בחר את "סטטוס התאימות" המתאים לכל דרישה. אם התשובה לאחת מן הדרישות היא "**לא**", הנך נדרש למלא את התאריך שבו תעמוד החברה בדרישה ולתאר בקצרה את הפעולות הננקטות על מנת לעמוד בדרישה. *בדוק מול חברת כרטיסי האשראי או מותגי(י) האשראי לפני מילוי חלק 4, הואיל ולא כל חברות מותגי האשראי דורשות חלק זה.*

דרישת PCI DSS	תיאור הדרישה	סטטוס תאימות (בחר אחד)		תאריך ופעולות תיקון (אם סטטוס התאימות שסומן הוא "לא")
		כן	לא	
3	הגן על הנתונים המאוחסנים של כרטיסי האשראי.	☐	☐	
4	הצפן את ההעברה של פרטי בעל הכרטיס על פני רשתות ציבוריות פתוחות.	☐	☐	
7	הגבל את הגישה לפרטי כרטיסי האשראי עפ"י העקרון של הצורך העסקי לדעת.	☐	☐	
9	הגבל את הגישה הפיזית לנתונים של כרטיסי האשראי.	☐	☐	
12	יישם ותחזק מדיניות המטפלת באבטחת מידע בקרב כלל כח האדם (עובדים וקבלנים).	☐	☐	