נציג בית העסק הנכבד,

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

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 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 C-VT (SAQ)
והצהרת תאימות

בתי עסק עם מסופי Web וירטואליים, 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 C-VT פותח עבור בתי עסק רלוונטיים המעבדים נתוני אשראי אך ורק באמצעות מסופים וירטואליים מבודדים על מחשבים אישיים המחוברים לאינטרנט.

מסוף וירטואלי הנו גישת רשת דרך הדפדפן לאתר חברת כרטיסי האשראי, לספק המעבד את התשלומים, או לספק צד שלישי על מנת לאשר עסקאות צד שלישי, כאשר בית העסק מזין ידני ת את פרטי האשראי באמצעות דפדפן המחובר בחיבור מאובטח. בשונה ממסופים פיזיים, מסופים וירטואליים לא קוראים נתונים ישירות מכרטיס האשראי. היות ונתוני האשראי מוזנים בצורה ידנית, נעשה שימוש במסופים וירטואליים במקום במסופים פיזיים בבתי עסק בעלי נפח עסקאות נמוך.

בתי העסק הללו מעבדים נתוני אשראי אך ורק דרך מסופים וירטואליים ואינם שומרים נתוני אשראי על אף אחת ממערכות המחשוב של הארגון. המסופים הווירטואליים הללו מחוברים לאינטרנט על מנת להתחבר לגורם צד שלישי אשר מארח את שירות עיבוד התשלום הווירטואלי. גורם צד שלישי זה יכול להיות, ספק המעבד תשלומים (processor), חברת כרטיסי האשראי או ספק צד שלישי אחר השומר, מעבד ו/או משדר נתוני אשראי על מנת לאשר ו/או לקיים עסקאות המתקבלות ממסוף התשלום הווירטואלי של בית העסק.

שאלון הערכה עצמית זה מיועד אך ורק לבתי עסק המזינים ידנית באמצעות מקלדת לתוך מסוף Web וירטואלי עסקה בודדת בכל פעם.

בתי עסק המתאימים למילוי שאלון הערכה עצמית C-VT , מעבדים נתוני אשראי באמצעות מסופים וירטואליים על מחשבים אישיים המחוברים לאינטרנט, הם לא שומרים נתוני אשראי על אף מחשב בארגון, ועשויים להיות בתי עסק (המבצעים עסקאות פנים מול פנים – כרטיס נוכח) או בתי עסק המבצעים עסקאות בטלפון/דואר (עסקאות כרטיס לא נוכח).

בתי עסק אלו מאשרים את עמידתם בתקן באמצעות מילוי שאלון C-VT, המאמתים כי:

- עבוד עסקאות בארגון מתבצע אך ורק דרך מסוף וירטואלי אשר הגישה אליו היא דרך האינטרנט באמצעות דפדפן.
- פתרון המסוף הווירטואלי של הארגון מסופק על ידי ספק צד שלישי אשר עומד בדרישות התקן PCI DSS.
- הארגון ניגש למסוף הווירטואלי העומד בדרישות ה PCI DSS באמצעות מחשב אשר מבודד במיקום אחד ויחיד ואינו מחובר למיקומים נוספים או למערכות אחרות בתוך הארגון (ניתן להשיג יעד זה באמצעות פיירוול או באמצעות סגמנטציה של הרשת שנועדה לבודד את המחשב מהמערכות האחרות בארגון).
- למחשב באמצעותו ניגשים למסוף הווירטואלי לא מחוברת חומרה שנועדה לשמור נתוני אשראי (למשל, קוראי כרטיסים המחוברים למחשב).
- על המחשב באמצעותו ניגשים למסוף הווירטואלי, לא מותקנות תוכנות הגורמות לנתוני האשראי להישמר (לדוגמא אין תוכנות, batch processing או תוכנות "שמור והעבר" – store-and forward).
- הארגון אינו מקבל או משדר בכל דרך אחרת נתוני אשראי בפורמט אלקטרוני (למשל דרך רשת פנימית או דרך האינטרנט).
- הארגון שומר אך ורק דוחות נייר או העתקי נייר של קבלות; ומסמכים אלו לא מועברים באופן אלקטרוני; 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".

גרסה מקוצרת זו של השאלון כוללת שאלות הנוגעות לסוג מסוים של בתי עסק קטנים, כפי שמוגדר בקריטריוני הסיווג לעיל. אם חלות על הסביבה שלך דרישות PCI DSS שאינן מופיעות בשאלון זה, זו עשויה להיות אינדיקציה לכך ששאלון זה אינו מתאים לסביבת העבודה שלך. בנוסף, עליך לעמוד בכל הדרישות הרלוונטיות של תקן PCI DSS על מנת לקבל סטטוס 'עומד בתקן PCI DSS'.

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

אף שרוב הארגונים הממלאים את שאלון C-VT יידרשו לאשרר את התאימות שלהם עם כל אחת מדרישות ה PCI DSS, חלק מהארגונים אשר פועלים במודלים עסקיים ספציפיים מאוד, עשויים לגלות שחלק מהדרישות אינן רלוונטיות עבורם. לדוגמה, לא מצופה מחברה אשר אינה עושה שימוש בטכנולוגיה אלחוטית כלשהי לאשרר תאימות עם דרישות PCI DSS ספציפיות הנוגעות לניהול טכנולוגיות אלחוטיות (דרישות 1.2.3, 2.1.1 ו-4.1.1, לדוגמה) .

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*ידרישות 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 C-VT

בית העסק מאשר כי סיווגו מתאים למילוי גרסה מקוצרת זו של שאלון הערכה עצמית מהנימוקים הבאים:

☐	עיבוד העסקאות של בית העסק מתבצע אך ורק באמצעות מסוף וירטואלי אליו ניגשים באמצעות דפדפן המחובר לאינטרנט.
☐	פתרון המסוף הווירטואלי מסופק ומתארח אצל ספק צד שלישי אשר עומד בתקן PCI DSS.
☐	בית העסק ניגש למסוף הווירטואלי באמצעות מחשב מבודד במיקום אחד בארגון ואינו מחובר למיקומים או מערכות אחרות בארגון.
☐	על המחשב באמצעותו ניגשים למסוף הווירטואלי, לא מותקנות תוכנות הגורמות לנתוני האשראי להישמר (לדוגמא אין תוכנות, batch processing או תוכנות "שמור והעבר" – store-and forward).
☐	למחשב באמצעותו ניגשים למסוף הווירטואלי לא מחוברת חומרה שנועדה לשמור נתוני אשראי (למשל, קוראי כרטיסים המחוברים למחשב).
☐	הארגון אינו מקבל או משדר בכל דרך אחרת נתוני אשראי בפורמט אלקטרוני (למשל דרך רשת פנימית או דרך האינטרנט).
☐	הארגון אינו שומר נתוני אשראי בפורמט אלקטרוני; ובנוסף
☐	אם הארגון שומר נתוני אשראי, הוא שומר אך ורק דוחות נייר או העתקי נייר של קבלות אשר אינן מתקבלות באופן אלקטרוני;

פרק 2: שאלון הערכה עצמית C-VT

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

תאריך מילוי הטופס:

בנה ותחזק רשת בטוחה

דרישה 1: התקנה ותחזוקה של Firewall בתצורה המגנה על נתוני כרטיסי האשראי

	שאלה	בדיקות נדרשות	תגובה(סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
1.2	האם קונפיגורצית ה – firewall והנתבים מגבילה את הגישה של רשתות לא אמינות לכל המערכות בסביבת נתוני כרטיסי האשראי כדלהלן: הערה: רשת לא אמינה הינה כל רשת חיצונית לרשתות השייכות לישות הנסקרת, ו/או מחוץ ליכולות השליטה או הניהול של הישות.						
1.2.1	א. האם התעבורה הנכנסת והיוצאת מוגבלת לזו ההכרחית לסביבת נתוני כרטיסי האשראי והאם הגבלות אלה מתועדות?	• עבור על הסטנדרטים של קונפיגורציו ת הנתב וה-firewall • בדוק את קונפיגורציו ת הנתב וה-firewall	☐	☐	☐	☐	☐
	ב. האם כל יתר התעבורה הנכנסת ויוצאת נחסמת באופן מפורש (למשל באמצעות חוק "deny all")?	• עבור על הסטנדרטים של קונפיגורציו ת הנתב וה-firewall • בדוק את קונפיגורציו ת הנתב וה-firewall	☐	☐	☐	☐	☐
1.2.3	האם הותקנו firewalls היקפיים בין כל הרשתות האלחוטיות וסביבת נתוני כרטיסי האשראי,	• עבור על הסטנדרטים של	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה(סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	והאם הוגדרו ה firewalls האלה לחסום כל תעבורה מהסביבה האלחוטית לסביבת נתוני כרטיסי האשראי או, אם תעבורה מסוג זה הכרחית לצורך עסקי, לאשר רק תעבורה מאושרת בין הסביבה האלחוטית לסביבת נתוני כרטיסי האשראי?	• בדוק את קונפיגורציו ת הנתב וה-firewall					
1.3	האם הגדרות ה – firewall אוסרות על גישה ציבורית ישירה בין האינטרנט לבין כל רכיבי המערכת בסביבת נתוני כרטיסי האשראי באופן הבא:						
1.3.3	האם נאסרת תעבורה ישירה – נכנסת ויוצאת בין האינטרנט לבין סביבת נתוני כרטיסי האשראי?	• בדוק את קונפיגורציו ת הנתב וה-firewall	☐	☐	☐	☐	☐
1.3.5	האם תעבורה היוצאת מסביבת נתוני כרטיסי האשראי לאינטרנט מאושרת באופן מפורש?	• בדוק את קונפיגורציו ת הנתב וה-firewall	☐	☐	☐	☐	☐
1.3.6	האם מיושמת בדיקת עומק (stateful inspection) הידועה גם כסינון חבילות מידע דינאמי (dynamic packet filtering) (כלומר רק חיבורים "מוכרים" מורשים ברשת)?	• בדוק את קונפיגורציו ת הנתב וה-firewall	☐	☐	☐	☐	☐
1.4	א. האם תוכנת firewall אישית הותקנה ופועלת על כל מכשיר נייד ו/או מכשירי עובדים בעלי חיבור ישיר לאינטרנט מחוץ לרשת (למשל מחשבים ניידים בשימוש העובדים) ואשר משמשים גם כדי להתחבר לרשת הארגונית?	• עבור על סטנדרטים של המדיניות והקונפיגורצ יה • בדוק מכשירים ניידים ו/או את מכשירי העובדים	☐	☐	☐	☐	☐
	ב. האם תצורת ה firewall האישיים מוגדרת בהתאם לנהלים ספציפיים, פועלת כעת, מורשים ולא ניתנת לשינוי על ידי משתמשי	• עבור על סטנדרטים של המדיניות והקונפיגורצ	☐	☐	☐	☐	☐

שאלה	בדיקות נדרשות	תגובה(סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
מכשירים ניידים ו/או מכשירי עובדי החברה?	יה • בדוק מכשירים ניידים ו/או את מכשירי העובדים					

דרישה 2: אין להשתמש בהגדרות ברירת מחדל של ספקים עבור סיסמאות מערכת ומרכיבי אבטחה אחרים

	שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
2.1	א. האם ברירות מחדל המוגדרות על ידי הספק מוחלפות תמיד טרם התקנת המערכת ברשת? *נקודה זו מתייחסת לכל סיסמאות ברירות המחדל, כולל אבל לא מוגבל לסיסמאות בשימוש במערכות הפעלה, תוכנה המספקת שירותי אבטחה, יישום וחשבונות מערכת, מסופים בנקודות מכירה, SNMP, וכו'.*	• עבור על מדיניות והליכים • בחן את מסמכי הספקים • בחן את קונפיגורציית המערכת והגדרות החשבון • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ב. האם חשבונות ברירת מחדל לא נחוצים הוסרו או נוטרלו לפני התקנת מערכת על הרשת?	• עבור על מדיניות והליכים • בחן את מסמכי הספקים • בחן את קונפיגורציית המערכת והגדרות החשבון • ראיין את כוח האדם	☐	☐	☐	☐	☐
2.1.1	האם בסביבות אלחוטיות המחוברות לסביבת נתוני כרטיסי אשראי, או המשדרות נתוני כרטיסים, כל ברירות המחדל האלחוטיות של הספק						

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
מוחלפות בעת ההתקנה באופן הבא:						
א. האם מפתחות ההצפנה מוחלפים מברירת המחדל בזמן ההתקנה ובכל פעם שמישהו בעל ידע על המפתחות עוזב את החברה או מחליף תפקיד?	• עבור על מדיניות והליכים • בחן את מסמכי הספקים • ראיין את כוח האדם	☐	☐	☐	☐	☐
ב. האם מוחלפת הגדרת ברירת המחדל של ה SNMP community strings במכשירים אלחוטיים בזמן ההתקנה?	• עבור על מדיניות והליכים • בחן מסמכי ספקים • בחן את קונפיגורציית המערכת והגדרות החשבון • ראיין את כוח האדם	☐	☐	☐	☐	☐
ג. האם הסיסמאות המוגדרות כברירת מחדל בכל נקודות הגישה מוחלפות בזמן התקנה?	• עבור על מדיניות והליכים • ראיין את כוח האדם • בדוק את קונפיגורציות המערכת	☐	☐	☐	☐	☐
ד. האם רכיב התוכנה בתוך החומרה של המכשיר האלחוטי מעודכן על מנת לתמוך בהצפנה חזקה לצורך זיהוי ושידור מעל רשתות אלחוטיות?	• עבור על מדיניות והליכים • בחן את מסמכי הספקים • בדוק את קונפיגורציות המערכת	☐	☐	☐	☐	☐
ה. האם ברירות מחדל אחרות המוגדרות על ידי הספק מוחלפות כשצריך?	• עבור על מדיניות והליכים • בחן את מסמכי הספקים • בדוק את קונפיגורציות	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		המערכת					
2.2.2	א. האם מאופשרת הפעילות רק של אותם שירותים, פרוטוקולים ודיימונים חיוניים באופן הנדרש לפעולתה של המערכת. (שירותים ופרוטוקולים שאינם נדרשים באופן ישיר על מנת לאפשר את פעולת המערכת מנוטרלים)?	• עבור על סטנדרטים של הקונפיגורציה • בחן את קונפיגורציית המערכת	☐	☐	☐	☐	☐
	ב. האם השימוש בכל השירותים, פרוטוקולים ודיימונים הלא בטוחים אשר פועלים, מוצדק ומיושמים לפי הסטנדרטים של הקונפיגורציה המתועדת?	• עבור על הסטנדרטים של הקונפיגורציה • ראיין את כוח האדם • בחן את הגדרות הקונפיגורציה • השווה בין שירותים וכן הלאה מאושרים לבין הצדקות מתועדות	☐	☐	☐	☐	☐
2.2.3	האם מאפייני אבטחה נוספים מתועדים ומיושמים עבור כל שירות, פרוטוקול או דיימון נחוצים הנחשבים ללא-בטוחים? (לדוגמה, טכנולוגיות אבטחה כמו SSH, FTP-S, SSL, IPSec או VPN מיושמות על מנת להגן על שירותים לא בטוחים כגון NetBios, שיתוף קבצים, Telnet, FTP וכו).	• עבור על הסטנדרטים של הקונפיגורציה • בחן את הגדרות הקונפיגורציה					
2.2.4	א. האם אדמיניסטרטור המערכת או האנשים האחראיים על קביעת תצורת רכיבי המערכת, הנם בעלי ידע בפרמטרים הנפוצים של הגדרת אבטחת המערכת?	• ראיין את כוח האדם	☐	☐	☐	☐	☐
	ב. האם הפרמטרים הנפוצים של הגדרת תצורת אבטחת המערכת כלולים בסטנדרטים של תצורת המערכת?	• בחן את הסטנדרטים של קונפיגורציית המערכת	☐	☐	☐	☐	☐
	ג. האם הפרמטרים של הגדרת	• בחן את מרכיבי	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	תצורת אבטחת המערכת, מיושמים כהלכה על כל רכיבי המערכת?	המערכת • בחן את הגדרות פרמטר האבטחה • השווה את ההגדרות לסטנדרטים של קונפיגורציית המערכת					
2.2.5	א. האם כל היישומים הלא הכרחיים כגון – סקריפטים, דרייברים, תכונות, תתי מערכות, מערכות קבצים ושרתי Web, הוסרו?	• בחן את פרמטרים האבטחה על מרכיבי המערכת	☐	☐	☐	☐	☐
	ב. האם היישומים הפועלים מתועדים והאם הם פועלים בתצורה מאובטחת?	• עבור על המסמכים • בחן את פרמטרים האבטחה על מרכיבי המערכת	☐	☐	☐	☐	☐
	ג. האם רק יישומים מתועדים קיימים ברכיבי המערכת?	• עבור על המסמכים בחן את פרמטרים האבטחה על מרכיבי המערכת	☐	☐	☐	☐	☐
2.3	האם גישת אדמיניסטרטור שלא דרך מסוף (non console admin access) מוצפנת כדלהלן: *השתמש בטכנולוגיות כגון SSH, VPN או TLS/SSL בשימוש בגישה ניהולית דרך האינטרנט או כאשר נעשה שימוש בממשקי גישה אדמיניסטרטיביים שלא דרך מסוף אחרים.*						
	א. האם כל גישת אדמיניסטרטור שלא דרך מסוף, מוצפנת באמצעות מנגנון הצפנה חזק, והאם ההצפנה מופעלת לפני שהאדמיניסטרטור מתבקש לספק את הסיסמה?	• בחן את רכיבי המערכת • בחן את קונפיגורציית המערכת • צפה במנהל נכנס למערכת	☐	☐	☐	☐	☐

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
ב. האם תצורת שירותי המערכת וקבצי פרמטרים נקבעה באופן שימנע שימוש ב Telnet או באמצעים לא בטוחים אחרים לגישה מרחוק?	• בחן את רכיבי המערכת • בחן שירותים וקבצים	☐	☐	☐	☐	☐
ג. האם גישת אדמיניסטרטור מהאינטרנט לממשקי ניהול מוצפנת באמצעות מנגנון הצפנה חזק?	• בחן את רכיבי המערכת • צפה במנהל נכנס למערכת	☐	☐	☐	☐	☐
ד. עבור הטכנולוגיה שבשימוש, האם מנגנון הצפנה חזק מיושם בהתאם לנהלים הטובים במשק (best practice) ו/או המלצות הספק?	• בחן את רכיבי המערכת • בחן את מסמכי הספקים • ראיין את כוח האדם					

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	ג. 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	☐	☐	☐	☐	☐
	ד. האם כל המערכות עונות לדרישות הבאות בנוגע לאי-שמירה של מידע אימות רגיש לאחר אישור עסקה (אפילו אם הוא מוצפן)?						
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	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		• 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 להצגה של נתוני מחזיקי כרטיסי אשראי – למשל דרישות סוג כרטיס תשלום או דרישות משפטיות בנוגע לקבלות בנקודות מכירה (POS).*	• עבור על המדיניות והנהלים • עבור על התפקידים שצריכים גישה לתצוגה מלאה של ה-PAN • בחן את קונפיגורציית 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
4.1	א. האם נעשה שימוש בהצפנה חזקה ובפרוטוקולי אבטחה כגון SSH ,TLS/SSL, IPSEC על מנת להגן על נתונים רגישים של כרטיסי אשראי במהלך שידור על פני רשתות ציבוריות פתוחות? *דוגמאות לרשתות ציבוריות פתוחות הרלוונטיות להקשר של תקן PCI DSS כוללות אך לא מוגבלות ל: אינטרנט; טכנולוגיות אלחוטיות כולל 802.11 ובלוטות'; טכנולוגיות סלולריות, כגון GSM, CDMA ו GPRS*	• עבור על סטנדרטים מתועדים • עבור על מדיניות והליכים • עבור על כל המקומות בהם CHD משודר או נקלט • בחן את קונפיגורציי ת המערכת	☐	☐	☐	☐	☐
	ב. האם מתקבלים רק מפתחות ו/או אישורים ממקור בטוח?	• צפה בתשדורות פנימה והחוצה • בחן מפתחות ואישורים	☐	☐	☐	☐	☐
	ג. האם פרוטוקולי האבטחה מיושמים אך ורק בתצורה מאובטחת ולא תומכים בגרסאות תצורה לא מאובטחות?	• בחן את קונפיגורציי ת המערכת	☐	☐	☐	☐	☐
	ד. האם מיושם חוזק הצפנה המתאים לשיטת ההצפנה שנעשה בה שימוש (בדוק את המלצות הספק/סטנדרטים מקובלים)?	• בחן את מסמכי הספקים • בחן את קונפיגורציי ת המערכת	☐	☐	☐	☐	☐
	ה. ליישומי TLS/SSL, האם SSL/TLS מאופשר כאשר נתוני מחזיקי כרטיסי אשראי	• בחן את קונפיגורציי ת המערכת	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
משודרים או מתקבלים? *לדוגמה, עבור יישומים מבוססי דפדפן:* • *האם בדפדפן מופיע HTTPS כחלק מכתובת האינטרנט (URL)?* • *האם נתוני כרטיסי אשראי נדרשים רק כאשר מופיע HTTPS בכתובת האינטרנט בדפדפן (URL)?*							
האם נעשה שימוש בנהלים מקובלים בתעשייה (למשל, IEEE 802 11i), כדי ליישם הצפנה חזקה של תהליכי אימות ושידור עסקאות ברשתות אלחוטיות שמשדרות נתוני כרטיסי אשראי או מחוברות לסביבת כרטיסי האשראי? ***הערה:*** *השימוש ב WEP כבקרת אבטחה אסור.*	4.1.1	• עבור על סטנדרטים מתועדים • עבור על רשתות אלחוטיות • בחן את קונפיגורציי ת המערכת	☐	☐	☐	☐	☐
ב. האם ישנם נהלים הקובעים כי אין לשלוח מספרי כרטיסי אשראי בלתי מוגנים באמצעות טכנולוגיות העברת מסרים של משתמשי קצה?	4.2	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐

דרישה 5: הגן על כל המערכות נגד תוכנות זדוניות ועדכן את תוכנת האנטי וירוס באופן קבוע

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
5.1	האם מותקנת תוכנת אנטי וירוס על כל המערכות שבדרך כלל מושפעות/עשויות להיפגע מתוכנות זדוניות?	• בחן את קונפיגורציית המערכת	☐	☐	☐	☐	☐
5.1.1	האם כל תוכנות האנטי-וירוס המותקנות מסוגלות לזהות, להסיר ולהגן מפני כל הסוגים הידועים של תוכנות זדוניות (לדוגמה, וירוסים, סוסים טרויאנים, תולעים, תוכנות ריגול, תוכנות פרסומת, וערכות ריגול (rootkit))?	• בחן את מסמכי הספקים • בחן את קונפיגורציית המערכת	☐	☐	☐	☐	☐
5.1.2	האם מתבצעות הערכות תקופתיות כדי לזהות ולהעריך איומים מתפתחים של תוכנות זדוניות על מנת לאשר שהמערכות שנחשבות כלא מושפעות מתוכנות זדוניות נשארות כאלו?	• ראיין את כוח האדם					
5.2	האם כל תוכנות האנטי וירוס מעודכנות, פועלות ומייצרות לוגים לבקרה (audit logs) כדלקמן:						
	א. האם נוהל האנטי-וירוס דורש עדכון של תוכנת האנטי-וירוס וההגדרות שלה?	• עבור על מדיניות והליכים • בחן את קונפיגורציי ת אנטי-וירוס, כולל את ההתקנה הראשית • בחן את רכיבי המערכת	☐	☐	☐	☐	☐
	ב. האם עדכונים	• בחן את	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	אוטומטים וסריקות תקופתיות מוגדרים כפעילים?	קונפיגורציי ת אנטי-וירוס, כולל את ההתקנה הראשית • בחן את רכיבי המערכת					
ג.	האם כל מנגנוני האנטי וירוס מייצרים לוגים לבקרה (Audit logs) והאם הלוגים נשמרים בהתאם לדרישה 10.7 לתקן PCI DSS?	• בחן את קונפיגורציות האנטי-וירוס • עבור על הלוגים של הליכי שימור	☐	☐	☐	☐	☐
5.3	האם כל המנגנונים נגד וירוסים: • פעילים? • בלתי ניתנים לכיבוי או שינוי על ידי המשתמשים? ***הערה:*** *ניתן לכבות זמנית פתרונות אנטי-וירוס רק במקרה של צורך טכנולוגי, כפי שמאושר על ידי ההנהלה על בסיס כל מקרה לגופו. אם יש צורך לבטל את הגנת האנטי-וירוס למטרה ספציפית, חייב להיות אישור רשמי. יתכן ויהיה צורך באמצעי אבטחה נוספים בזמן שהגנת האנטי-וירוס לא פעילה.*	• בחן את קונפיגורציות האנטי-וירוס • בחן את רכיבי המערכת • צפה בהליכים • ראיין את כוח האדם					

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
6.1	**האם ישנו תהליך שנועד לזהות נקודות תורפה באבטחה כולל:** • **שימוש במקורות חיצוניים אמינים עבור מידע על נקודות תורפה?** • **דירוג רמת סיכון לנקודות תורפה הכולל זיהוי כל נקודות התורפה בעלות סיכון "גבוה" ו-"קריטי"?** **הערה: דירוג הסיכונים צריך להיות מבוסס על סטנדרטים מקובלים בתעשייה כמו גם על התחשבות בהשפעה פוטנציאלית. לדוגמה, קריטריונים לדירוג נקודות תורפה יכולים לכלול הסתמכות על הציון הבסיסי ב- CVSS ו/סיווג על ידי הספק ו/או סוג המערכות שיושפעו.** **שיטות להערכת נקודות תורפה ודיורג הסיכונים ישתנו בהתאם לסביבת הארגון ואסטרטגיית הערכת הסיכונים שלו. לכל הפחות, הערכת סיכונים צריכה לזהות את כל נקודות התורפה הנחשבות לבעלות "סיכון גבוה" לסביבה. בנוסף לדירוג הסיכון, נקודות תורפה יכולות להיחשב "קריטיות" אם הן מהוות איום מיידי לסביבה, משפיעות על מערכות קריטיות, ו/או יגרמו לבעיית אבטחה פוטנציאלית אם לא יוטפלו. דוגמאות למערכות קריטיות כוללות מערכות אבטחה, מכשירים ומערכות הנמצאים בקשר עם הציבור, מאגרי מידע ומערכות אחרות המאחסנות, מעבדות או משדרות נתוני מחזיקי כרטיסי אשראי.**	• עבור על מדיניות והליכים • ראיין את כוח האדם • צפה בהליכים	☐	☐	☐	☐	☐
6.2	א. **האם כל רכיבי המערכת והתוכנה מוגנים מפני חשיפה לנקודת תורפה ידועות באמצעות התקנה של טלאי האבטחה (patches)**	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
המעודכנים ביותר של הספק?						
ב. האם טלאי האבטחה (patches) מותקנים בתוך חודש אחד מיום פרסומם? **הערה: יש לזהות טלאי אבטחה קריטיים לפי תהליך דירוג רמת סיכון המתואר בדרישה 6.1**	• עבור על מדיניות והליכים • בחן רכיבי מערכת • השווה בין רשימת טלאי האבטחה המותקנים לבין רשימות הטלאים העדכניות	☐	☐	☐	☐	☐

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 מאובטחיסבאופן 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
12.1	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 והעובדים בעלי הגישה?	▪ עקוב אחר מדיניות	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		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	☐	☐	☐	☐	☐
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	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		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 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	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		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.*

פרק 3 – אישור ואימות פרטים

חלק 3. אישור PCI DSS

בהסתמך על התוצאות שהתקבלו בשאלון C-VTמתאריך *(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 C-VT 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	
1	התקן ותחזק Firewall בתצורה המגנה על נתוני כרטיסי האשראי.	☐	☐	
2	אין להשתמש בהגדרות ברירת מחדל של ספקים עבור סיסמאות מערכת ומרכיבי אבטחה אחרים.	☐	☐	
3	הגן על הנתונים המאוחסנים של כרטיסי האשראי.	☐	☐	
4	הצפן את ההעברה של פרטי בעל הכרטיס על פני רשתות ציבוריות פתוחות.	☐	☐	
5	הגן על כל המערכות נגד תוכנות זדוניות ועדכן את תוכנת האנטי וירוס באופן קבוע.	☐	☐	
6	פתח ותחזק מערכות ואפליקציות מאובטחות.	☐	☐	
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).	☐	☐	