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 (SAQ) D
והצהרת תאימות לבתי עסק

שאלון לכל היתר – בתי עסק

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

שינויי מסמך iii
לפני שמתחילים v
הערכה עצמית PCI DSS – שלבי ביצוע v
הבנת שאלון ההערכה העצמית v
מילוי שאלון ההערכה העצמית vi
הנחיה בנוגע לחוסר הרלוונטיות של דרישות ספציפיות מסוימות vi
החרגה משפטית vii
פרק 1 – פרטי ההערכה 8
פרק 2 – שאלון הערכה עצמית D לבתי עסק 11
בנה ותחזק רשת בטוחה 11
דרישה 1: התקנה ותחזוקה של Firewall בתצורה המגנה על נתוני כרטיסי האשראי 11
דרישה 2: אין להשתמש בהגדרות ברירת מחדל של ספקים עבור סיסמאות מערכת ומרכיבי אבטחה אחרים 18
הגנה על נתוני אשראי 25
דרישה 3: הגן על הנתונים המאוחסנים של כרטיסי האשראי 25
דרישה 4: הצפן את השידור של נתוני כרטיסי אשראי על פני רשתות ציבוריות פתוחות 33
יישם ותחזק תוכנית לניהול נקודות תורפה 36
דרישה 5: הגן על כל המערכות נגד תוכנות זדוניות ועדכן את תוכנת האנטי וירוס באופן קבוע 36
דרישה 6: פתח ותחזק מערכות ואפליקציות מאובטחות 38
הטמע אמצעי בקרת גישה חזקים 47
דרישה 7: הגבל את הגישה לפרטי כרטיסי האשראי עפ"י העקרון של הצורך העסקי לדעת 47
דרישה 8: זהה ואשר גישה לרכיבי מערכת 51
דרישה 9: הגבל את הגישה הפיזית לנתונים של כרטיסי אשראי 60
בצע ניטור ובדיקה של הרשת באופן קבוע 71
דרישה 10: נטר ועקוב אחר כל גישה למשאבי הרשת ולנתוני כרטיסי האשראי 71
דרישה 11: בצע בדיקות שוטפות של מערכות ותהליכי האבטחה 80
יישם ותחזק מדיניות אבטחת מידע 91
דרישה 12: יישם ותחזק מדיניות הנותנת מענה לאבטחת מידע בקרב כלל כח האדם (עובדים וקבלנים) 91
נספח א': דרישות נוספות עבור ספקי אירוח משותף (Providers Shared Hosting) 102
נספח ב': גיליון בקרות מפצות 103
נספח ג': הסבר על חוסר רלוונטיות (N/A) 104
נספח ד': הסבר על דרישות שלא נבחנו (Not Tested) 105
פרק 3 – אישור ואימות פרטים 106

Copyright 2014 PCI Security Standards Council LLC

לפני שמתחילים

שאלון הערכה עצמית D לסוחרים חל על כל נותני השירות ובתי העסק המתאימים אשר אינם עונים לדרישות הסיווג של שאלוני הערכה עצמית אחרים. דוגמאות לסביבות מסחר המתאימות להגדרות הסיווג של שאלון D עשויות לכלול, ללא הגבלה:

- סוחרים במסחר אלקטרוני המקבלים נתוני כרטיסי אשראי באתר האינטרנט שלהם
- סוחרים המחזיקים מאגרי מידע אלקטרוניים של נתוני כרטיסי אשראי
- סוחרים שאינם מחזיקים נתוני כרטיסי אשראי בצורה אלקטרונית, אך אינם עומדים בדרישות הסיווג של שאלוני הערכה עצמית אחרים
- סוחרים בסביבות העומדות בדרישות הסיווג של שאלוני הערכה עצמית אחרים, אולם קיימות דרישות PCI DSS נוספות החלות על סביבת המסחר שלהם

אף שרוב הארגונים הממלאים את שאלון D יידרשו לאשרר את התאימות שלהם עם כל אחת מדרישות ה PCI DSS, חלק מהארגונים אשר פועלים במודלים עסקיים ספציפיים, עשויים לגלות שחלק מהדרישות אינן רלוונטיות עבורם. ראה ההנחיות להלן לקבלת מידע בנוגע להוצאת דרישות ספציפיות אל מחוץ לחובת אשרור התאימות.

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

Copyright 2014 PCI Security Standards Council LLC

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 D 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. באופן דומה, ארגון שאינו מאחסן בשום שלב נתונים של מחזיקי כרטיס אשראי בצורה אלקטרונית, לא נדרש לאשרר את הדרישות הנוגעות לאחסון מאובטח של נתוני כרטיסי אשראי (דרישה 3.4, לדוגמה).

דוגמאות לדרישות בעלות רלוונטיות ספציפית:

Copyright 2014 PCI Security Standards Council LLC

- יש לענות על שאלות ספציפיות באשר לאבטחת טכנולוגיות אלחוטיות (דרישות 1.2.3, 2.1.1 ו-4.1.1, לדוגמה) אך ורק במידה וקיימת תקשורת אלחוטית ברשת הארגון. יש להביא בחשבון שדרישה 11.1 (שימוש בתהליכים לזיהוי נקודות גישה אלחוטיות לא מורשות) חייבת להתמלא גם במידה והארגון אינו עושה שימוש בטכנולוגיות אלחוטיות, היות ומטרת תהליך זה היא לאתר רכיבים זדוניים בלתי מורשים אשר עשויים להיות מותקנים בארגון ללא ידיעת בית העסק.
- יש לענות על השאלות הנוגעות לפיתוח יישומים וכתיבת קוד בצורה מאובטחת (דרישות 6.3 ו-6.5) רק במידה ובית העסק מפתח אפליקציות ייחודיות המותאמות עבורו.
- יש לענות על השאלות בדרישות 9.1.1 ו-9.3 רק בנוגע למתקנים בהם קיימים "אזורים רגישים" כפי שמוגדר כאן: "אזורים רגישים" הינם אזורים שבהם קיים מרכז נתונים כלשהו, חדר שרתים או כל אזור אחר המאכלס מערכות המאחסנות, מעבדות או משדרות נתוני כרטיסי אשראי. זאת להוציא אזורים בהם קיימים רק מסופי נקודות מכירה (POS), כמו למשל אזור הקופות בחנות, אך כולל את חדר השרתים של החנות המאחסן את נתוני כרטיסי האשראי ואת אזורי האחסון בהם כמויות גדולות של נתוני כרטיסי אשראי.

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.

הבנת ההבדל בין האפשרות 'לא רלוונטי' לאפשרות 'לא נבחן'

דרישות שנראה כי אינן רלוונטיות לסביבה מסוימת יש לאשרר ככאלה. בהמשך לדוגמה שהובאה לעיל בנוגע לאי-שימוש בטכנולוגיות אלחוטיות, אם ארגון בוחר באפשרות "לא רלוונטי" לגבי דרישות 1.2.3, 2.1.1 ו-4.1.1, עליו לאשר תחילה כי לא קיימות טכנולוגיות אלחוטיות בסביבת נתוני כרטיסי האשראי שלו או המתחברות לסביבת נתוני האשראי. רק לאחר אישור עובדה זו, יכול הארגון לבחור באפשרות "לא רלוונטי" לדרישות ספציפיות אלה.

במקרים שבהם דרישה כלשהי אינה נבחנת כלל והשאלה *האם* היא רלוונטית אינה נשקלת, יש לבחור באפשרות "לא נבדק". להלן דוגמאות למצבים שבהם אפשרות זו מתרחשת:

- ארגון נתבקש על-ידי חברת כרטיסי האשראי שאתה הוא עובד לאשרור רק חלק מסוים מדרישות התקן – לדוגמה: שימוש בגישת התעדופים לאשרור אבני דרך ספציפיות.
- ארגון מבקש לאשרר בקרת אבטחה חדשה המשפיעה רק על חלק מדרישות התקן – לדוגמה, הטמעת שיטת הצפנה חדשה הדורשת הערכה של דרישות 2, 3 ו-4 של תקן PCI DSS.
- ספק שירותים מציע שירות המכסה רק מספר מוגבל של דרישות PCI DSS – לדוגמה, ספק שירתי אחסון פיזיים מבקש לאשרר רק את בקרות האבטחה הפיזיות בדרישה 9 של PCI DSS במתקן האחסון שלו.

בתרחישים אלה, הארגון מבקש לאשרר רק דרישות PCI DSS מסוימות גם אם דרישות אחרות חלות על סביבת המסחר שלו.

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:			

Copyright 2014 PCI Security Standards Council LLC

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

Copyright 2014 PCI Security Standards Council LLC

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.*

Copyright 2014 PCI Security Standards Council LLC

פרק 2 – שאלון הערכה עצמית D לבתי עסק

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
1.1	האם הסטנדרטים הקיימים והמיושמים בקונפיגורציית ה firewall והנתבים (routers) כוללים את הדברים הבאים:						
1.1.1	האם יש תהליך רשמי לאישור ובחינת כל חיבורי הרשת החיצוניים והשינויים לקונפיגורצית ה – firewall והנתבים?	• עבור על התהליך המתועד • ראיין את כוח האדם • בדוק את קונפיגורציו ת הרשת	☐	☐	☐	☐	☐
1.1.2	א. האם ישנו תרשים רשת עדכני המתעד את כל החיבורים בין סביבת נתוני כרטיסי אשראי לרשתות אחרות, לרבות רשתות אלחוטיות?	• עבור על תרשים הרשת העדכנית • בדוק את קונפיגורציו ת הרשת	☐	☐	☐	☐	☐
	ב. האם ישנו הליך לוודא שהתרשים יישאר עדכני?	• ראיין את כוח האדם האחראי	☐	☐	☐	☐	☐
1.1.3	א. האם יש תרשים עדכני המראה את כל הנתוני כרטיסי האשראי על פני מערכות ורשתות?	• עבור על תרשים זרימת המידע הנוכחי • בדוק את	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה			בדיקות נדרשות	תגובה(סמן תגובה אחת לכל שאלה)				
				כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
			קונפיגורציו ת הרשת					
		ב. האם ישנו הליך לוודא שהתרשים ישאר עדכני?	• ראיין את כוח האדם	☐	☐	☐	☐	☐
1.1.4		א. האם הגדרות הקונפיגורציה כוללת דרישה ל firewall לכל חיבור אינטרנט וכן בין כל אזור מפורז (DMZ) לאזור הרשת הפנימית?	• עבור על סטנדרט הקונפיגורצי ה של ה-Firewall • בחן את קונפיגורציי ת הרשת כדי לוודא שה-firewall במקום	☐	☐	☐	☐	☐
		ב. האם תרשים הרשת הקיים תואם את הגדרות התצורה של ה firewall?	• השווה את סטנדרטים קונפיגורציי ת ה-firewall עם תרשים הרשת הנוכחי	☐	☐	☐	☐	☐
1.1.5		האם הסטנדרטים של קונפיגורצית ה firewall והנתבים (routers) כוללים את תיאור הקבוצות, התפקידים ותחומי אחריות בניהול הלוגי של רכיבי הרשת?	• עבור על הסטנדרטים של קונפיגורציו ת הנתב וה-firewall • ראיין את כוח האדם	☐	☐	☐	☐	☐
1.1.6		א. האם הסטנדרטים של קונפיגורצית ה firewall והנתבים (routers) כוללים רשימה מתועדת של כל השירותים, הפרוטוקולים וערוצי התקשורת (ports), לרבות הצדקה עסקית (לדוגמה פרוטוקולים	• עבור על הסטנדרטים של קונפיגורציו ת הנתב וה-firewall	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה(סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	מסוג SSL HTTP, SSH, VPN).						
	ב. האם זוהו כל השירותים, הפרוטוקלים וערוצי התקשורת (ports) הבלתי מאובטחים והאם ישנם אמצעי אבטחה מתועדים ומיושמים עבור כל אחד מהם? *הערה: דוגמאות לשירותים, פרוטוקולים או ערוצי תקשורת בתלי מאובטחים כוללים בין היתר FTP, Telnet, POP3, IMAP ו- SNMP*	• עבור על הסטנדרטים של קונפיגורציו ת הנתב וה- firewall • בדוק את קונפיגורציו ת הנתב וה- firewall	☐	☐	☐	☐	☐
1.1.7	א. האם הסטנדרטים של קונפיגורצית ה firewall והנתבים (routers) דורשים ביצוע בדיקה של מערך חוקי ה – firewall והנתבים כל שישה חודשים לפחות?	• עבור על הסטנדרטים של קונפיגורציו ת הנתב וה- firewall	☐	☐	☐	☐	☐
	ב. האם מערך חוקי ה firewall והנתבים נבדקים כל שישה חודשים לפחות?	• בדוק מסמכים מביקורות ה- firewall	☐	☐	☐	☐	☐
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	• עבור על הסטנדרטים של קונפיגורציו ת הנתב וה-	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה(סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	הגבלות אלה מתועדות?	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	☐	☐	☐	☐	☐
1.2.2	האם קבצי הקונפיגורציה של הנתבים מאובטחים מפני גישה בלתי מאובטחת ומסונכרנים - לדוגמה, הרצה של הקונפיגורציה (או קונפיגורציה פעילה) תואמת את קונפיגורציית ההפעלה (המשמשת כאשר מדליקים את המכשירים)?	• עבור על הסטנדרטים של קונפיגורציו ת הנתב וה- firewall • בדוק את קבצי קונפיגורציי ת הנתב ואת קונפיגורציי ת הנתב	☐	☐	☐	☐	☐
1.2.3	האם הותקנו firewalls היקפיים בין כל הרשתות האלחוטיות וסביבת נתוני כרטיסי האשראי, והאם הוגדרו 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?	• עבור על הסטנדרטים של קונפיגורציו ת הנתב וה- firewall • 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:						

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה(סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
1.3.1	האם הוקם DMZ להגבלת התעבורה הנכנסת רק לרכיבי מערכת המספקים שירותים, פרוטוקולים וערוצי תקשורת (ports) מורשים לגישה ציבורית?	• בדוק את קונפיגורציו ת הנתב וה-firewall	☐	☐	☐	☐	☐
1.3.2	האם תעבורת האינטרנט הנכנסת מוגבלת לכתובות IP שנמצאות בתוך ה DMZ?	• בדוק את קונפיגורציו ת הנתב וה-firewall	☐	☐	☐	☐	☐
1.3.3	האם נאסרת תעבורה ישירה – נכנסת ויוצאת בין האינטרנט לבין סביבת נתוני כרטיסי האשראי?	• בדוק את קונפיגורציו ת הנתב וה-firewall	☐	☐	☐	☐	☐
1.3.4	האם יושמו אמצעים נגד-spoofing כדי לזהות לחסום כתובת IP ממקור מזויף מכניסה לרשת? (לדוגמה, לחסום תעבורה המגיעה מהרשת עם כתובת פנימית.)	• 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	☐	☐	☐	☐	☐
1.3.7	האם רכיבי המערכת המחזיקים את נתוני הכרטיסים (כמו בסיסי נתונים) ממוקמים בתוך הרשת הפנימית בנפרד מה-DMZ ומרשתות בלתי אמינות אחרות?	• בדוק את קונפיגורציו ת הנתב וה-firewall	☐	☐	☐	☐	☐
1.3.8	א. האם יושמו שיטות למניעת חשיפתם של כתובות IP פרטיות ומידע הניתוב לאינטרנט?	• בדוק את קונפיגורציו ת הנתב וה-firewall	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה(סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
הערה: שיטות להסתרת כתובות IP יכולות לכלול אבל לא מוגבלות לשיטות הבאות: • תרגום כתובות רשת – NAT • מיקום שרתים המכילים נתוני כרטיסי אשראי מאחורי שרתי פרוקסי (proxy servers)/ firewall או מטמוני תוכן (content caches) • הסרה או סינון של פרסום הנתיב של רשתות פרטיות המשתמשות כתובות רשומות (registered addressing) • שימוש פנימי ב RFC1918 address space במקום בכתובות רשומות.						
ב. האם ישנו אישור לכל חשיפה של כתובות IP פרטית ומידע ניתוב לישויות חיצוניות?	• בדוק את קונפיגורציו ת הנתב וה-firewall • ראיין את כוח האדם	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה(סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
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 והקונפיגורציה • 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 מכשירים ניידים ו/או מכשירי עובדי החברה?	• עבור על סטנדרטים של המדיניות והקונפיגורציה • בדוק מכשירים ניידים ו/או את מכשירי העובדים	☐	☐	☐	☐	☐
1.5	האם מדיניות האבטחה ונהלי הפעולה לניהול ה- firewall: • מתועדים • בשימוש • ידועים לכל הצדדים הרלוונטיים?	• עבור על מדיניות האבטחה ונהלי הפעולה • ראיין את כוח האדם	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

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 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	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	במכשירים אלחוטיים בזמן ההתקנה?	• 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 המערכת	☐	☐	☐	☐	☐
2.2 א.	האם נקבעו נהלים להגדרת תצורה לכל רכיבי המערכת והאם הם תואמים לסטנדרטים המקובלים בתעשייה בנוגע להקשחת מערכות? *מקורות לסטנדרטים מקובלים בתעשייה להקשחת מערכות כוללים בין היתר אבל לא רק את, SysAdmin Audit Network (SANS), National*	• עבור על סטנדרטים קונפיגורציית הרשת • עבור על הסטנדרטים המקובלים בתעשייה להקשחת מערכות • עבור על מדיניות	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
Institute of Standards Technology (NIST), International Organization for Standardization (ISO), Center of Internet Security (CIS).	והליכים • ראיין את כוח האדם					
ב. האם הסטנדרטים להגדרת תצורת המערכת מתעדכנים כאשר מתגלות נקודות תורפה חדשות כמוגדר בדרישה 6.1?	• עבור על מדיניות והליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
ג. האם פועלים על פי הסטנדרטים להגדרת תצורת מערכת כאשר מוגדרת מערכת חדשה?	• עבור על מדיניות והליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
ד. האם הסטנדרטים להגדרת תצורת מערכת כוללים את הדברים הבאים: • החלפת כל ברירות המחדל המסופקות על ידי הספק והסרת כל חשבונות ברירת המחדל המיותרים? • יישום פעולה מרכזית אחת בלבד בכל שרת כדי למנוע מצב בו פעולות הדורשות רמת אבטחה שונה נמצאות יחד על אותו שרת? • מתן אישור רק לשירותים, פרוטוקולים, דיימונים, וכו' כפי הנדרש לתפקוד המערכת? • יישום מאפייני אבטחה נוספים עבור שירותים, פרוטוקולים או דיימונים נצרכים הנחשבים בלתי-מאובטחים? • תצורת פרמטרים של אבטחת המערכת כדי	• עבור על הסטנדרטים של קונפיגורציות המערכת					

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	למנוע שימוש לא ראוי? • הסרת תפעולים לא הכרחיים כגון תוכנות script, כוננים, מאפיינים, תתי-מערכות, מערכות קבצים, ושרתי רשת לא נחוצים?						
2.2.1	א. האם ישנו ייעוד שימוש עיקרי אחד לכל שרת על מנת למנוע מצב בו ייעודי שימוש שונים הדורשים רמת אבטחה שונה מתקיימים על אותו שרת? (לדוגמה, שרתי web, שרתי database, ושרתי DNS צריכים להיות מוקמים על שרתים נפרדים).	• בחן את קונפיגורציית המערכת	☐	☐	☐	☐	☐
	ב. אם נעשה שימוש בטכנולוגיית וירטואליזציה, האם ישנו ייעוד שימוש עיקרי אחד לכל רכיב או מערכת וירטואלית?	• בחן את קונפיגורציית 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,	• עבור על הסטנדרטים של					

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	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).	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 תצורת אבטחת המערכת, מיושמים כהלכה על כל רכיבי המערכת?	• בחן את מרכיבי 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	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

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

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
2.4	א. האם יש רשימת מצאי עבור רכיבי המערכת שבשימוש עבור PCI DSS, כולל רשימה של רכיבי חומרה ותוכנה ותיאור של השימוש של כל אחד?	• בחן את מצאי המערכת	☐	☐	☐	☐	☐
	ב. האם המצאי המתועד עדכני?	• ראיין את כוח האדם	☐	☐	☐	☐	☐
2.5	האם מדיניות האבטחה ונהלי הפעולה לניהול ברירות מחדל של הספק ופרמטרים אחרים של אבטחה: • מתועדים • בשימוש ידועים לכל הצדדים הרלוונטיים?	• עבור על מדיניות האבטחה ונהלי הפעולה • ראיין את כוח האדם	☐	☐	☐	☐	☐
2.6	*דרישה זו רלוונטית רק לספקים השירות*						

Copyright 2014 PCI Security Standards Council LLC

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
3.1	האם המדיניות והנהלים של שימור והשמדה (data retention and disposal) של מידע כוללים את הדברים הבאים:						
	א. האם כמות אכסון המידע ושמירתו מוגבלים לזמן הנדרש למטרות עסקיות, חוקיות ו/או רגולטוריות?	• עבור על מדיניות ונהלים של שימור והשמדה • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ב. הנוגעות האם יש תהליכים מוגדרים לגבי השמדה מאובטחת של המידע כאשר הוא כבר לא נדרש מטעמים עסקיים, חוקיים או רגולטורים?	• עבור על המדיניות וההליכים • ראיין את כוח האדם • בחן את מנגנון ההשמדה	☐	☐	☐	☐	☐
	ג. האם יש דרישות שמירה ספציפיות עבור נתוני מחזיקי כרטיס אשראי? *לדוגמה, נתוני כרטיסי אשראי צריכים להישמר למשך תקופה X בגלל סיבות עסקיות Y .*	• עבור על המדיניות וההליכים • ראיין את כוח האדם • בחן את דרישות השמירה	☐	☐	☐	☐	☐
	ד. האם יש הליך רבעוני לזיהוי והשמדה מאובטחת של נתוני מחזיקי כרטיסי אשראי שמורים החורגים מהדרישות המוגדרות לשמירה?	• עבור על המדיניות וההליכים • ראיין את כוח האדם • צפה בתהליכי השמדה	☐	☐	☐	☐	☐
	ה. האם כל נתוני כרטיסי האשראי המאוחסנים עונים לדרישות המוגדרות במדיניות שימור המידע?	• בחן קבצים ותיעוד של המערכת	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
3.2	א. *הליך בדיקה זה שייך רק למנפיקים*						
	ב. *הליך בדיקה זה שייך רק למנפיקים*						
	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)?						
3.2.1	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* *על מנת לצמצם את הסיכון, שמור רק את הפרטים הללו כאשר יש צורך עסקי בכך.*	• בחן מקורות מידע כולל: • מידע נכנס על עסקאות • כל הרשומות • קבצי היסטוריה • קבצי ערוצים • סכמת מאגר המידע • תוכן מאגר המידע	☐	☐	☐	☐	☐
3.2.2	האם הקוד (CVC) או ערך הקוד (CVV) לאימות הכרטיס (המספר בעל שלוש או ארבע ספרות המודפס בקדמת	• בחן מקורות מידע כולל:	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
או בגב הכרטיס) אינו נשמר לאחר האימות?		• מידע נכנס על עסקאות • כל הרשומות • קבצי היסטוריה • קבצי ערוצים • סכמת מאגר המידע • תוכן מאגר המידע					
האם מספר הזיהוי האישי (PIN) או בלוק מידע הכולל את ה PIN המוצפן אינם נשמרים לאחר האימות?	3.2.3	• בחן מקורות מידע כולל: • מידע נכנס על עסקאות • כל הרשומות • קבצי היסטוריה • קבצי ערוצים • סכמת מאגר המידע • תוכן מאגר המידע	☐	☐	☐	☐	☐
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)*	3.3	• עבור על המדיניות והנהלים • עבור על התפקידים שצריכים גישה לתצוגה מלאה של ה-PAN • בחן את קונפיגורציית המערכת • צפה בתצוגות של PAN	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
3.4	האם מספר כרטיס האשראי משובש בצורה שאינה ניתנת לקריאה בכל מקום בו הוא מאוחסן (כולל במאגרי מידע, מדיה דיגיטלית ניידת, מדיה לגיבוי ולוגים לבקרה (audit logs)) באמצעות אחת מהשיטות הבאות? ▪ תמצית (hashes) חד כיוונית המבוססת על הצפנה חזקה (התמצית תעשה על כל מספר כרטיס האשראי). ▪ קיצוץ (truncation) (לא ניתן להשתמש בתמצית (hash) להחלפת החלק המקוצץ של מספר הכרטיס). ▪ מצביעים ואסימונים (יש לשמור את האסימונים באופן מאובטח).הצפנה חזקה עם תהליכים ונהלים נלווים לניהול מפתחות ההצפנה. *הערה: אדם שכוונתיו זדוניות נדרש למאמץ קטן יחסית כדי לשחזר את נתוני הכרטיס המקוריים אם יש לו גישה הן לגרסה המגובבת והן לגרסה המקוצצת של מספר כרטיס האשראי. במקרה שקיימות גרסה מגובבת ומקוצצת של אותו מספר כרטיס בסביבה של ישות כלשהי, יש להתקין בקרות נוספות על מנת להבטיח שלא ניתן לקשר בין הגרסה המגובבת לגרסה המקוצצת של מספר הכרטיס האשראי לצורך שחזור המספר המלא.*	• בחן את מסמכי הספקים • בחן את אחסון המידע • בחן את המדיה הניתנת להסרה • בחן תיעוד בקרות	☐	☐	☐	☐	☐
3.4.1	אם נעשה שימוש בהצפנה ברמת הדיסק (להבדיל מהצפנה ברמת הקובץ או ברמת עמודה בבסיס הנתונים) האם הגישה מנוהלת באופן הבא:						
	א. האם הגישה הלוגית למערכות של קבצים מוצפנים מנוהלת באופן נפרד ועצמאי ממנגנוני בקרת הגישה הבסיסיים של מערכת ההפעלה המקומית (לדוגמה, על ידי הימנעות משימוש בבסיסי הנתונים של חשבון המשתמש המקומי או אישורי כניסה לרשת כללית)?	• בחן את קונפיגורציית המערכת • צפה בהליך אימות	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	ב. האם מפתחות ההצפנה מאוחסנים בצורה מאובטחת (לדוגמה, מאוחסנים על גבי מדיה ניידת המוגנת באמצעות מנגנוני הגבלת גישה חזקים)?	• צפה בהליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ג. האם נתוני כרטיסי אשראי תמיד מוצפנים על גבי מדיה ניידת? ***הערה:*** *אם לא נעשה שימוש בהצפנה ברמת הדיסק להצפנה של מדיה ניידת, יש להפוך את הנתונים שמצויים על גבי מדיה זו לבלתי קריאים באמצעות שיטה אחרת.*	• בחן את קונפיגורציית המערכת • צפה בהליכים	☐	☐	☐	☐	☐
3.5	האם כל המפתחות שנעשה בהם שימוש לאבטחת נתוני כרטיסי אשראי מוגנים מפני חשיפה ושימוש לרעה באופן הבא: ***הערה:*** *דרישה זו חלה על מפתחות הצפנה המשמשים להגנה על מפתחות הצפנה של נתונים -- מפתחות הצפנה עיקריים כגון אלה צריכים להיות חזקים לפחות כמו מפתח ההצפנה של הנתונים.*						
3.5.1	האם הגישה למפתחות ההצפנה מוגבלת למספר הקטן ביותר ההכרחי של ממונים/אחראים?	• בחן רשימות גישה למשתמשים	☐	☐	☐	☐	☐
3.5.2	האם מפתחות הצפנה סודיים ופרטיים המשמשים להצפנה/ פענוח נתונים של מחזיקי כרטיסי אשראי מאוחסנים באחד (או יותר) מהצורות הבאות בכל זמן? • מוצפנים עם מפתח הצפנה למפתחות שחזק לפחות כמו מפתח הצפנת מידע, ושמאוחסן בנפרד ממפתח הצפנת המידע • בתוך מכשיר הצפנה מאובטח (כגון מודלת אבטחה מארח (HSM) או מכשיר מאושר PTS בנקודת השקה) • בעל לפחות שני רכיבי הצפנה עיקריים באורך מלא או שיתוף מפתחות, בהתאם לשיטה	• עבור על התהליך המתועד • בחן את קונפיגורציות המערכת ומקומות אחסון מפתחות ההצפנה, כולל מפתחות ההצפנה למפתחות ההצפנה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	המקובלת בתעשייה ***הערה:*** *לא נדרש שהמפתחות הציבוריים יאוחסנו באחת מהצורות הללו.*		☐	☐	☐	☐	☐
3.5.3	האם מפתחות הצפנה מאוחסנים במספר הקטן ביותר האפשרי של מקומות אחסון?	• בחן מקומות אחסון מפתחות הצפנה • צפה בהליכים	☐	☐	☐	☐	☐
3.6	א. האם המדיניות וכל הנהלים לניהול מפתחות ההצפנה המשמשים להצפנה של נתוני כרטיסי אשראי מתועדים ומיושמים במלואם?	• עבור על הליכי ניהול המפתחות	☐	☐	☐	☐	☐
	ב. *הליך בדיקה זה מתייחס לספקי שירות בלבד.*						
	ג. האם המדיניות והנהלים של ניהול המפתחות המיושמים דורשים את הדברים הבאים:						
3.6.1	האם הנהלים הקשורים במפתחות המוצפנים כוללים ייצור של מפתחות הצפנה חזקים?	• עבור על הליכי ניהול המפתחות • צפה בשיטה לייצור מפתחות	☐	☐	☐	☐	☐
3.6.2	האם הנהלים הקשורים במפתחות המוצפנים כוללים הפצה מאובטחת של מפתחות ההצפנה?	• עבור על הליכי ניהול המפתחות • צפה בשיטת הפצת המפתחות	☐	☐	☐	☐	☐
3.6.3	האם הנהלים הקשורים במפתחות המוצפנים כוללים אחסון מאובטח של מפתחות ההצפנה?	• עבור על הליכי ניהול המפתחות • צפה בשיטת האחסון המאובטח של המפתחות	☐	☐	☐	☐	☐
3.6.4	האם הנהלים הקשורים במפתחות המוצפנים כוללים החלפת מפתחות הצפנה שהגיעו לסוף תקופת ההצפנה המוגדרת שלהם (למשל, אחרי שעבר פרק זמן מסוים ו/או אחרי שכמות מסוימת של טקסט מוצפן הופקה), כפי	• עבור על הליכי ניהול המפתחות • ראיין את כוח האדם	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	שהוגדרה על ידי יצרן האפליקציה הרלוונטית או בעל המפתח תוך התבססות על הנחיות וסטנדרטים מקובלים בתעשייה (לדוגמה NIST Special Publication 800-57)?						
3.6.5	א. האם הנהלים הקשורים במפתחות המוצפנים כוללים הפסקת שימוש או החלפה (למשל, ארכוב, השמדה ו/או ביטול) של מפתחות ההצפנה לפי הצורך כאשר אמינותם נחלשת (למשל עזיבה של עובד עם ידע לגבי מפתח הצפנה עם טקסט גלוי (clear-text key))?	• עבור על הליכי ניהול המפתחות • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ב. האם הנהלים הקשורים במפתחות המוצפנים כוללים החלפה של מפתחות הידועים או חשודים ככאלה שנחשפו?	• עבור על הליכי ניהול המפתחות • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ג. אם מפתחות אשר הופסק בהם השימוש או הוחלפו, נשמרים – האם מפתחות אלה משמשים אך ורק לצרכי פענוח/אימות (decryption) (ולא משמשים לצורכי הצפנה)?	• עבור על הליכי ניהול המפתחות • ראיין את כוח האדם	☐	☐	☐	☐	☐
3.6.6	עבור פעילויות ניהול ידני של מפתחות הצפנה עם טקסט גלוי (clear text key) - האם הנהלים הקשורים במפתחות המוצפנים כוללים פיצול ידע ושליטה דואלית על מפתחות ההצפנה כדלקמן: ▪ האם הליכי ידע מפוצל דורשים שרכיבי המפתח יהיו בשליטת לפחות שני אנשים שלכל אחד יש מידע רק על רכיבי המפתח שאצלו? **ו-** ▪ האם הליכי שליטה דואלית דורשים לפחות שני אנשים כדי לבצע פעולות ניהול מפתחות כלשהן, ולאף אדם בודד אין גישה למרכיבי האימות (לדוגמה סיסמאות או מפתחות) של האחר?	• עבור על הליכי ניהול המפתחות • ראיין את כוח האדם ו/או • צפה בהליכים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	הערה: *דוגמאות לפעולות ניהול ידניות של מפתחות כוללות, אך אינן מוגבלות ל: יצירת מפתחות, העברה, טעינה, אחסון והשמדה.*						
3.6.7	האם הנהלים הקשורים במפתחות המוצפנים כוללים מניעת החלפה לא מורשית של מפתחות ההצפנה?	• עבור על ההליכים • ראיין את כוח האדם ו/או • צפה בהליכים	☐	☐	☐	☐	☐
3.6.8	האם הממונים על מפתחות ההצפנה נדרשים להכיר בצורה רשמית (בכתב או באופן אלקטרוני) שהם מבינים ומקבלים על עצמם את האחריות כממונים על המפתחות?	▪ עבור על ההליכים ▪ עבור על מסמכים או עדות אחרת	☐	☐	☐	☐	☐
3.7	האם מדיניות האבטחה ונהלי הפעולה עבור הגנה על מידע מחזיקי כרטיסי אשראי מאוחסן: • מתועדים • בשימוש • ידועים לכל הצדדים הרלוונטיים?	• עבור על מדיניות האבטחה ונהלי הפעולה ▪ ראיין את כוח האדם	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

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 TLS/SSL, SSH, 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	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

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)?*						
4.1.1	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.*	• עבור על סטנדרטים מתועדים • עבור על רשתות אלחוטיות • בחן את קונפיגורציי ת המערכת	☐	☐	☐	☐	☐
4.2 א.	האם מספרי כרטיסי האשראי מוגנים בהצפנה חזקה או שמוצגים כבלתי קריאים כל אימת שהם נשלחים דרך טכנולוגיות העברת מסרים של משתמשי קצה (לדוגמה, אימייל, תוכנת מסרים מידיים	• צפה בהליכים • עבור על תשדירים כלפי חוץ	☐	☐	☐	☐	☐

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
וצ'אט)?						
ב. האם ישנם נהלים הקובעים כי אין לשלוח מספרי כרטיסי אשראי בלתי מוגנים באמצעות טכנולוגיות העברת מסרים של משתמשי קצה?	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
4.3 האם מדיניות אבטחה ונהלי הפעולה להצפנת תשדורות של נתוני מחזיקי כרטיסי אשראי: • מתועדים • בשימוש • ידועים לכל הצדדים הרלוונטיים?	• עבור על מדיניות האבטחה ונהלי הפעולה • ראיין את כוח האדם					

Copyright 2014 PCI Security Standards Council LLC

יישם ותחזק תוכנית לניהול נקודות תורפה

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:						
	• 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	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

	שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	• האם עדכונים אוטומטים וסריקות תקופתיות מוגדרים כפעילים?	• בחן את קונפיגורציי ת אנטי-וירוס, כולל את ההתקנה הראשית • בחן את רכיבי המערכת	☐	☐	☐	☐	☐
	• 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					
5.4	האם מדיניות אבטחה ונהלי הפעולה להגנה על המערכות מפני תוכנות זדוניות: • מתועדים • בשימוש • ידועים לכל הצדדים הרלוונטיים?	• עבור על מדיניות האבטחה ונהלי הפעולה • ראיין את כוח האדם					

Copyright 2014 PCI Security Standards Council LLC

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 ודירוג 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	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

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	☐	☐	☐	☐	☐
6.3	א. האם תהליכי פיתוח התוכנה מבוססים על הוראות סטנדרטים מקובלים בתעשייה?	• עבור על הליכי פיתוח תוכנה • צפה בהליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ב. האם אבטחת מידע משולבת בכל שלב של מחזור חיי הפיתוח?	• עבור על הליכי פיתוח תוכנה • צפה בהליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ג. האם יישומי התוכנה מפותחים בהתאם לדרישות של תקן PCI DSS (למשל, אימות ותיעוד מאובטחים (secure authentication and logging))?	• עבור על הליכי פיתוח תוכנה • צפה בהליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ד. האם תהליכי פיתוח התוכנה כוללים את הדברים הבאים?						
6.3.1	האם פיתוח, בדיקה, ו/או כל החשבונות, סיסמאות, ושמות משתמשים הפנימיים מוסרים מהאפליקציה לפני שהיישום/אפליקציה הופכת לפעילה או מופצת ללקוחות?	• עבור על הליכי פיתוח תוכנה • ראיין את כוח האדם	☐	☐	☐	☐	☐
6.3.2	האם כל שינויי הקוד באפליקציה המפותחת נבדקים (באמצעות תהליכים ידניים או אוטומטים)	• עבור על הליכי פיתוח תוכנה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	לפני שחרור הגרסה או הפצה ללקוחות, על מנת לזהות נקודות תורפה פוטנציאליות בקוד כדלקמן: • האם שינויי הקוד נבדקים על ידי בודקים אשר אינם אלו שכתבו את הקוד ואשר הינם בקיאים בטכניקות של בדיקת קוד ונהלי כתיבת קוד מאובטח? • האם בדיקות הקוד מוודאות כי הקוד נכתב בהתאם להוראות כתיבת קוד מאובטח? • האם התיקונים הנדרשים מיושמים לפני שחרור הגרסה? • האם התוצאות של בדיקת הקוד נבדקות ומאושרות על ידי ההנהלה לפני שחרור הגרסה? ***הערה**: דרישה זו לבדיקות קוד חלה על כל פיתוח עצמי של קוד (הן לצרכים פנימיים והן לשימוש ציבורי חיצוני), כחלק ממחזור הפיתוח של המערכת. את בדיקות הקוד יכולים לערוך עובדים פנימיים המחזיקים בידע הדרוש או גורמים חיצוניים. אפליקציות Web הנגישות לציבור חיצוני כפופות ליישום של בקרות נוספות, וזאת על מנת לתת מענה לנקודות תורפה איומים מתמשכים גם לאחר הטמעת המערכת, כפי שמוגדר בדרישה 6.6 של PCI DSS.*	• ראיין את כוח האדם • בחן שינויים אחרונים ושנה את התיעוד					
6.4	האם דרישות תהליכי ונהלי 'בקרת שינויים' עבור שינויים ברכיבי המערכת, כוללות את הדברים הבאים:						
6.4.1	א. האם סביבות הפיתוח/בדיקות מופרדות מסביבת הייצור,	• עבור על הליכי ונהלי בקרת שינויים • בחן את תיעוד הרשת וקונפיגורציות	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		מכשירי הרשת					
	ב. האם קיימת בקרת גישה אשר אוכפת את ההפרדה בין סביבת הפיתוח/ בדיקות לבין סביבת הייצור?	• עבור על הליכי ונהלי בקרת שינויים • בחן הגדרות בקרת גישה					
6.4.2	האם יש הפרדה בין תחומי האחריות של אנשים העובדים בסביבת הפיתוח/בדיקות לתחומי האחריות של אנשים העובדים בסביבת הייצור?	• עבור על הליכי ונהלי בקרת שינויים • צפה בהליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
6.4.3	האם **לא** נעשה שימוש בנתוני סביבת ייצור (מספרי כרטיסי אשראי אמיתיים) לצורכי פיתוח או בדיקות?	• עבור על הליכי ונהלי בקרת שינויים • צפה בהליכים • ראיין את כוח האדם • בחן את נתוני המבדק	☐	☐	☐	☐	☐
6.4.4	האם חשבונות שנוצרו לצורך הבדיקות כמו גם כל הנתונים האחרים הקשורים בבדיקות, מוסרות מהמערכות לפני שהן הופכות לפעילות בסביבת הייצור?	• עבור על הליכי ונהלי בקרת שינויים • צפה בהליכים • ראיין את כוח האדם • בחן את מערכות המוצר	☐	☐	☐	☐	☐
6.4.5	א. האם נהלי בקרת שינויים להתקנת טלאי אבטחה ועדכוני תוכנה מתועדים וכוללים את הדרישות הבאות? • תיעוד ההשפעה • תיעוד אישור בקרת שינויים על ידי גוף מוסמך • בדיקת פונקציונליות כדי לוודא שהשינוי לא משפיע	• עבור על הליכי ונהלי בקרת שינויים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	בצורה שלילית על האבטחה של המערכת • הליכי חזרה (back out)						
	ב. האם הדרישות הבאות מקוימות ומתועדות עבור כל שינוי:						
6.4.5.1	תיעוד ההשפעה?	• עקוב אחר שינויים בתיעוד בקרת שינויים • בחן את תיעוד בקרת שינויים	☐	☐	☐	☐	☐
6.4.5.2	אישור מתועד (של השינוי) על ידי הגורמים המוסמכים בארגון?	• עקוב אחר שינויים בתיעוד בקרת שינויים • בחן את תיעוד בקרת שינויים	☐	☐	☐	☐	☐
6.4.5.3	א. בדיקת פונקציונאליות על מנת לוודא שלשינוי אין השפעה רעה על רמת הבטיחות של המערכת?	• עקוב אחר שינויים בתיעוד בקרת שינויים • בחן את תיעוד בקרת שינויים	☐	☐	☐	☐	☐
	ב. עבור עדכוני קוד בפיתוח עצמי – האם העדכונים נבדקים לתאימות עם דרישה 6.5 של PCI DSS לפני שהם עוברים לסביבת הייצור?	• עקוב אחר שינויים בתיעוד בקרת שינויים • בחן את תיעוד בקרת שינויים	☐	☐	☐	☐	☐
6.4.5.4	האם ישנם נהלי שחזור (back-out) עבור כל שינוי?	• עקוב אחר שינויים בתיעוד בקרת שינויים • בחן את תיעוד בקרת שינויים	☐	☐	☐	☐	☐
6.5	א. האם תהליכים לפיתוח תוכנה לוקחים בחשבון נקודות תורפה שכיחות בכתיבת קוד?	• עבור על הליכי ונהלי פיתוח תוכנה	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	ב. האם המפתחים בקיאים בטכניקות כתיבת קוד מאובטח, כולל איך להימנע מנקודות תורפה שכיחות בכתיבת קוד והבנה כיצד מידע רגיש מטופל בזיכרון?	• ראיין את כוח האדם • בחן את מסמכי ההכשרה	☐	☐	☐	☐	☐
	ג. האם תהליכי פיתוח התוכנה כוללים מניעת הימצאותן של נקודות תורפה בקוד על מנת לוודא שהאפליקציות אינן חשופות לכל הפחות ל: *הערה: נקודות התורפה המופיעות בסעיפים 6.5.1 עד 6.5.10 הינן מעודכנות בהתאם לסטנדרטים המקובלים בתעשייה נכון ליום פרסום גרסה זו של תקן PCI DSS. אולם היות והסטנדרטים בתעשייה מתעדכנים באופן שוטף, (למשל מדריך OWASP, SANS CWE Top 25, CERT Secure Coding ועוד) יש להשתמש בסטנדרטים המעודכנים ביותר בעת מילוי אחר דרישות אלה.*						
6.5.1	האם טכניקות כתיבת קוד מתייחסות לבעיות הזרקות קוד (Injection), ובמיוחד SQL Injection? ***הערה:*** *יש גם להיזהר מפני OS Command injection, LDAP ו XPath injections, כמו גם הזרקות קוד אחרות.*	• בחן תהליכי ונהלי פיתוח תוכנה • ראיין את כוח האדם	☐	☐	☐	☐	☐
6.5.2	האם טכניקות כתיבת קוד מתייחסות לנקודות תורפה של הצפת חוצץ? (Buffer Overflow)	• בחן תהליכי ונהלי פיתוח תוכנה • ראיין את כוח האדם	☐	☐	☐	☐	☐
6.5.3	האם טכניקות כתיבת קוד מתייחסות לאחסון מוצפן לא מאובטח של נתונים? (Insecure cryptographic	• בחן תהליכי ונהלי פיתוח תוכנה	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	storage)	• ראיין את כוח האדם					
6.5.4	האם טכניקות כתיבת קוד מתייחסות לתקשורת לא מאובטחת?	• בחן תהליכי ונהלי פיתוח תוכנה • ראיין את כוח האדם	☐	☐	☐	☐	☐
6.5.5	האם טכניקות כתיבת קוד מתייחסות לטיפול לא תקין בשגיאות? (improper error handling)	• בחן תהליכי ונהלי פיתוח תוכנה • ראיין את כוח האדם	☐	☐	☐	☐	☐
6.5.6	האם טכניקות כתיבת קוד מתייחסות לכל נקודות התורפה בעלות רמת סיכון "**גבוהה**" בתהליך זיהוי חשיפה לנקודת תורפה (כמוגדר בדרישה 6.2 ל PCI DSS)?	• בחן תהליכי ונהלי פיתוח תוכנה • ראיין את כוח האדם	☐	☐	☐	☐	☐
	עבור אפליקציות Web וממשקי אפליקציות (פנימיים או חיצוניים) האם אפליקציות מפותחות על בסיס הנחיות לכתיבת קוד מאובטח כדי להגן על אפליקציות מנקודות התורפה הנוספות הבאות:						
6.5.7	האם טכניקות כתיבת קוד מתייחסות לנקודות תורפה של Cross Site Scripting (XSS)?	• בחן תהליכי ונהלי פיתוח תוכנה • ראיין את כוח האדם	☐	☐	☐	☐	☐
6.5.8	האם טכניקות כתיבת קוד מתייחסות לבקרת גישה בלתי הולמת (improper access control) כגון, הפניות ישירות לא מאובטחות לאובייקטים (insecure direct object references), כשל בהגבלת גישה ל URL, מעבר לא מורשה בין ספריות וכשל בהגבלת גישת משתמשים לפעולות?	• בחן תהליכי ונהלי פיתוח תוכנה • ראיין את כוח האדם	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
6.5.9	האם טכניקות כתיבת קוד מתייחסות לבקשות מזויפות מאתרים אחרים Cross-site request forgery (CSRF)?	• בחן תהליכי ונהלי פיתוח תוכנה • ראיין את כוח האדם	☐	☐	☐	☐	☐
6.5.10	האם טכניקות כתיבת קוד מתייחסות לתהליכי אישור וניהול זמני פעילות פגומים? ***הערה**: דרישה 6.5.10 מהווה המלצה עד ל-30 ביוני, 2015. לאחר מכן היא תהפוך לדרישה*	• בחן תהליכי ונהלי פיתוח תוכנה • ראיין את כוח האדם	☐	☐	☐	☐	☐
6.6	האם באפליקציות Web הנגישות לציבור חיצוני מטופלים איומים ונקודות תורפה באופן שוטף, והאם האפליקציות האלה מוגנות מפני התקפות ידועות באמצעות *אחת* מהשיטות הבאות? ▪ סקירת אפליקציות ה-web הנגישות לציבור חיצוני באמצעות שיטות או כלים, ידניים או אוטומטיים, להערכת סיכוני אבטחה כדלקמן: ○ לפחות אחת לשנה ○ לאחר כל שינוי ○ על ידי ארגון שמתמחה באבטחת מידע ○ שכל נקודות התורפה (בקוד) מתוקנות ○ שהאפליקציה נסקרת	• עבור על תהליכים מתועדים • ראיין את כוח האדם • בחן את המסמכים של הערכות אבטחת אפליקציות • בחן את הגדרות קונפיגורציית המערכת	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	מחדש לאחר התיקונים ***הערה:*** *הערכה זו לא זהה לבדיקות נקודות התורפה המבוצעות עבור דרישה 11.2* -או- ▪ התקנת פתרון טכני אוטומטי המזהה ומונע התקפות מבוססות רשת (כגון firewall ברמת האפליקציה) לפני יישומי web הנגישים לציבור כדי למנוע לנטר את התעבורה כל הזמן.						
6.7	האם מדיניות אבטחה ונהלי הפעולה פיתוח ותחזוקת מערכות ואפליקציות מאובטחות: • מתועדים • בשימוש • ידועים לכל הצדדים הרלוונטיים?	• עבור על מדיניות האבטחה ונהלי הפעולה • ראיין את כוח האדם					

Copyright 2014 PCI Security Standards Council LLC

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:						
	האם יש מדיניות כתובה עבור בקרת גישה המשלבת את הנקודות הבאות? • הגדרת צרכי גישה ונתינת הרשאה מסווגת לכל תפקיד • זכויות הגישה של משתמשים מורשים היא בהתאם לרמת ההרשאות המינימלית הנדרשת להם לצורך ביצוע תפקידם • הקצאת גישה על בסיס סיווג התפקיד והתפקוד של העובד • אישור מתועד (אלקטרוני או בכתב) על ידי הגופים המוסמכים עבור כל גישה, כולל רישום הזכויות הספציפיות	• בחן מדיניות בקרת גישה כתובה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		דרישות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	שאושרו						
7.1.1	תפקידם האם דרישות הגישה עבור כל תפקיד מוגדרות כולל: • רכיבי מערכת ומקורות נתונים אליהם בעל התפקיד צריך גישה כדי למלא את תפקידו? • הרמה של הגישה הנדרשת (לדוגמה, משתמש, מנהל וכו') למקורות?	• בחן תפקידים וצרכי גישה	☐	☐	☐	☐	☐
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	☐	☐	☐	☐	☐
7.1.4	האם נדרש אישור מתועד מאת הגורמים המוסמכים המפרט את ההרשאות הנדרשות?	• עבור על מספרי המשתמש • השווה עם אישורים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		דרישות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		מתועדים • השווה בין הרשאות מוקצות לבין אישורים מתועדים					
7.2	האם במערכות עם מספר משתמשים קיימת מערכת בקרת גישה המגבילה את הגישה על בסיס הצורך של המשתמש להכיר את המידע, והאם הגדרת ברירת המחדל של המערכת היא "חסום הכל" (deny all) כל עוד לא הוגדר אחרת, כדלקמן:						
7.2.1	האם מערכות בקרת הגישה מכסות את כל רכיבי המערכת?	• בחן את מסמכי הספקים • בחן את הגדרות הקונפיגורציה	☐	☐	☐	☐	☐
7.2.2	האם מערכות בקרת הגישה מוגדרות לאכוף את ההרשאות המשתמשים בהתאם לסיווג העבודה והתפקיד?	• בחן את מסמכי הספקים • בחן את הגדרות הקונפיגורציה	☐	☐	☐	☐	☐
7.2.3	האם הגדרת ברירת המחדל של מערכות בקרת הגישה היא "חסום הכל" (deny all)?	• בחן את מסמכי הספקים • בחן את הגדרות הקונפיגורציה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		דרישות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		יה					
7.3	האם מדיניות אבטחה ונהלי הפעולה להגבלת גישה לנתוני כרטיסי אשראי: • מתועדים • בשימוש • ידועים לכל הצדדים הרלוונטיים?	• עבור על מדיניות האבטחה ונהלי הפעולה • ראיין את כוח האדם	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
8.1	האם אשראי תהליכים ונהלים לזיהוי משתמשים ובקרת ניהול מוגדרים ומיושמים עבור משתמשים שאינם צרכנים ומנהלים בנוגע לכל רכיבי המערכת, כדלקמן:						
8.1.1	האם מספר זיהוי ייחודי מוקצה לכל משתמש לפני אישור גישה לרכיבי מערכת או נתוני כרטיסי אשראי?	• עבור על תהליכי סיסמאות • ראיין את כוח האדם	☐	☐	☐	☐	☐
8.1.2	האם קיימים אמצעי בקרה על ההוספה, המחיקה והעדכון של מזהי משתמש, פרטי משתמש ואובייקטים אחרים המשמשים לזיהוי המשתמש, כך שהשימוש במזהי משתמש נעשה רק כפי שאושר (כולל אלה עם הרשאות מיוחדות)?	• עבור על תהליכי סיסמאות • בחן זיהוי משתמש מסווג וכללי ואישורים דומים • צפה בהגדרות המערכת	☐	☐	☐	☐	☐
8.1.3	האם הגישה למשתמשים שנפסלו נשללת מיידית?	• עבור על תהליכי סיסמאות • בחן חשבונות משתמשים שבוטלו • עבור על רשימות גישה מעודכנות • צפה במכשירי אימות פיזיים מוחזרים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
8.1.4	האם חשבונות משתמשים לא פעילים מעל 90 יום מוסרים או מוקפאים?	• עבור על תהליכי סיסמאות • צפה בחשבונות משתמשים	☐	☐	☐	☐	☐
8.1.5	א. האם חשבונות המשמשים ספקים לגישה, תמיכה או תחזוקה של רכיבי המערכת דרך גישה מרחוק מאופשרים רק למשך הזמן הדרוש ומנוטרלים כאשר הם לא בשימוש?	• עבור על תהליכי סיסמאות • ראיין את כוח האדם • צפה בהליכים	☐	☐	☐	☐	☐
	ב. האם חשבונות ספקים בגישה מרחוק מנוטרים כאשר הם בשימוש?	• ראיין את כוח האדם • צפה בהליכים	☐	☐	☐	☐	☐
8.1.6	א. האם ניסיונות גישה כושלים מוגבלים על ידי חסימת זיהוי המשתמש לאחר לא יותר משישה ניסיונות?	• עבור על תהליכי סיסמאות • בחן את הגדרות קונפיגורציית המערכת	☐	☐	☐	☐	☐
	ב. הליך בדיקה זה מתייחס רק לספקים						
8.1.7	לאחר שחשבון משתמש ננעל, הם תקופת הנעילה מוגדרת למינימום של 30 דקות או עד שמנהל מערכת מבטל את הנעילה?	• עבור על תהליכי סיסמאות • בחן את הגדרות קונפיגורציית המערכת	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
8.1.8	אם חשבון משתמש לא פעיל למשך יותר מ 15 דקות, האם המשתמש נדרש לבצע אימות מחדש (למשל, להזין מחדש את הסיסמה), על מנת להפעיל מחדש את החשבון?	• עבור על תהליכי סיסמאות • בחן את הגדרות קונפיגורציית המערכת	☐	☐	☐	☐	☐
8.2	בנוסף להקצאת זיהוי משתמש ייחודי, האם מיושמת לפחות אחת מהשיטות הבאות לאימות של כל המשתמשים? ▪ משהו שאתה יודע, כגון סיסמא ▪ משהו שיש לך, כגון אסימון אבטחה (token) או כרטיס חכם (smart card) ▪ משהו שאתה, כגון זיהוי ביומטרי	• עבור על תהליכי סיסמאות • צפה בתהליכי אישור	☐	☐	☐	☐	☐
8.2.1	א. האם כל הסיסמאות הופכות לבלתי קריאות במהלך שידורן ושמירתן בכל רכיבי המערכת באמצעות הצפנה חזקה?	• עבור על תהליכי סיסמאות • בחן את מסמכי הספקים • בחן את הגדרות קונפיגורציית המערכת • צפה בקבצי סיסמאות • צפה בשידור נתונים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	ב. הליך בדיקה זה מתייחס רק לספקים						
8.2.2	האם זהות המשתמש מאומתת לפני שינויים בנתוני האימות (לדוגמה, שינוי סיסמא, הקצאת אסימון אבטחה חדש, או ייצור מפתחות אבטחה חדשים)?	• עבור על הליכי אימות • צפה בעובדים	☐	☐	☐	☐	☐
8.2.3	א. האם הפרמטרים של סיסמאות משתמשים מחייבים שהסיסמאות יעמדו בתנאים הבאים? • אורך סיסמא של לפחות 7 תווים ? • הסיסמאות חייבות להכיל גם תווים נומריים (ספרות) וגם תווים אלפביתיים (אותיות)? לחלופין, הסיסמאות חייבות להיות מורכבות ובעלות חוזק לפחות כמו התנאים לעיל.	• בחן הגדרות קונפיגורציית המערכת לאימות הפרמטרים לסיסמאות	☐	☐	☐	☐	☐
	ב. הליך בדיקה זה מתייחס רק לספקים						
8.2.4	א. האם סיסמאות המשתמשים מוחלפות לפחות פעם ב 90 יום?	• עבור על תהליכי סיסמאות • בחן את הגדרות קונפיגורציית המערכת	☐	☐	☐	☐	☐
	ב. הליך בדיקה זה מתייחס רק לספקים						
8.2.5	א. האם בעת בחירת סיסמא חדשה, משתמש נדרש לבחור סיסמא אשר שונה	• עבור על תהליכי סיסמאות	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	מארבע הסיסמאות האחרונות שלו?	• דגום את רכיבי המערכת • בחן את הגדרות קונפיגורציית המערכת					
	ב. הליך בדיקה זה מתייחס רק לספקים						
8.2.6	האם סיסמאות ראשוניות וסיסמאות לאחר איפוס הינן בעלות ערך ייחודי עבור כל משתמש, והאם כל משתמש מחויב לשנות אותן מיד לאחר השימוש הראשון?	• עבור על תהליכי סיסמאות • בחן את הגדרות קונפיגורציית המערכת • צפה בעובדי האבטחה	☐	☐	☐	☐	☐
8.3	האם שילוב של שני גורמי אימות (Two-Factor Authentication) מיושם עבור גישה מרחוק (גישה ברמת הרשת ממקום הנמצא מחוץ לרשת) של עובדים, מנהלי מערכת וגורמים אחרים (כולל גישת ספקים עבור תמיכה או תחזוקה)?). ***הערה:*** *אימות כפול דורש ששתיים מתוך שלוש שיטות האימות (ר' דרישה 8.2 לתיאור שיטות האימות) ישמשו לאימות. שימוש באותה שיטה פעמיים (למשל שימוש בשתי סיסמאות נפרדות) אינו נחשב אימות כפול.* *דוגמאות לאימות כפול כוללות שירות חיוג ואימות מרחוק (RADIUS) עם tokens או בקרת גישה באמצעות מסוף Access*	• עבור על מדיניות והליכים • בחן את קונפיגורציית המערכת • צפה בעובדים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	Controller Access Control System (TACACS) עם tokens; או טכנולוגיות אחרות המיישמות אימות כפול.						
8.4	א. האם מדיניות ונהלי האימות (authentication) מועברים לכל המשתמשים אשר יש להם גישה לנתוני כרטיסי אשראי?	• עבור על מדיניות והליכים • עבור על שיטת ההפצה • ראיין את כוח האדם • ראיין משתמשים	☐	☐	☐	☐	☐
	ב. האם תהליכי ונהלי אישור כוללים את: • הדרכה לבחירת אמצעי אימות חזקים • הדרכה על כיצד על משתמשים להגן על אמצעי האימות שלהם • הנחיות לא להשתמש מחדש בסיסמאות ישנות • הנחיות שעל המשתמשים לשנות סיסמאות אם עולה חשד שהסיסמה לא בטוחה	• עבור על מדיניות והליכים • עבור על המסמכים המסופקים למשתמשים	☐	☐	☐	☐	☐
8.5	האם סיסמאות וחשבונות קבוצתיים, כלליים או משותפים אסורים לשימוש כדלקמן: ▪ חשבונות ומזהי משתמשים כלליים מוקפאים או מוסרים; ▪ מזהי משתמש משותפים לפעולות אדמיניסטרטיביות						

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	ופעולות קריטיות אחרות אינם קיימים; ובנוסף לא ניתן לבצע פעולות אדמיניסטרציה על שום רכיב במערכת באמצעות מזהי משתמש משותפים וכלליים.						
8.5.1	הליך בדיקה זה מתייחס רק לספקים						
8.6	כאשר נעשה שימוש במנגנוני אימות אחרים (לדוגמה, אסימוני אבטחה לוגיים או פיזיים, כרטיסים חכמים ותעודות וכו') האם השימוש במנגנונים אלו מוקצה כלהלן? • מנגנוני אימות חייבים להיות מוקצים לחשבון מסוים ולא משותפים למספר חשבונות • בקרות לוגיות ו/או פיזיות חייבות להתקיים כדי לוודא שרק החשבון המיועד משתמש במנגנון לקבלת גישה	• עבור על מדיניות והליכים • ראיין את כוח האדם • בחן את הגדרות קונפיגורציית המערכת ו/או בקרות פיזיות	☐	☐	☐	☐	☐
8.7	האם גישה לכל בסיס נתונים המכיל נתוני כרטיסי אשראי (כולל גישה על ידי יישומים, מנהלי מערכת וכל משתמש אחר) מוגבלת כדלקמן:						
א.	האם גישה לשאילתות משתמשים ולפעולות משתמשים (כגון, העבר, העתק, מחק) בבסיס הנתונים מתבצעת באמצעות מתודות מתוכנתות בלבד (למשל, stored procedures)?	• עבור על מדיניות והליכים של אימות מאגר המידע • בחן את הגדרות הקונפיגורציה של מאגר	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		המידע ויישומים					
ב.	האם גישה ישירה לבסיס הנתונים או ביצוע שאילתות מול בסיס הנתונים מוגבלת למנהלי בסיס הנתונים?	• עבור על מדיניות והליכים של אימות מאגר המידע • בחן את הגדרות הגישה למאגר המידע • בחן את הגדרות הקונפיגורציה של אפליקציית מאגר המידע	☐	☐	☐	☐	☐
ג.	האם מזהי אפליקציות בעלות גישה לבסיס הנתונים יכולים להיות רק בשימוש האפליקציות (ולא בשימוש של משתמשים או תהליכים אחרים)?	• עבור על מדיניות והליכים של אימות מאגר המידע • בחן את הגדרות הגישה למאגר המידע • בחן את הגדרות הקונפיגורציה של אפליקציית מאגר המידע	☐	☐	☐	☐	☐
8.8	האם מדיניות אבטחה ונהלי הפעולה לזיהוי ואימות: • מתועדים • בשימוש	• עבור על מדיניות האבטחה ונהלי הפעולה					

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
• ידועים לכל הצדדים הרלוונטיים?	• ראיין את כוח האדם					

Copyright 2014 PCI Security Standards Council LLC

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
9.1	האם נעשה שימוש בבקרות כניסה נאותות למתקנים על מנת להגביל ולנטר את הגישה הפיזית למערכות הנתונים של כרטיסי האשראי?	• צפה בבקרת הגישה הפיזית • צפה בעובדים	☐	☐	☐	☐	☐
9.1.1	א. האם נעשה שימוש במצלמות אבטחה ו/או מנגנוני בקרת גישה אחרים כדי לפקח על הגישה הפיזית של אנשים לאזורים רגישים? ***הערה:*** "אזור רגיש" מתייחס לכל מרכז מידע (data center), חדר שרתים, או כל אזור אחר המאכלס מערכות השומרות נתוני כרטיסי אשראי. הגדרה זו אינה חלה על אזור בו נמצאים רק מסופי נקודות מכירה כגון אזור הקופות הרושמות בחנות.	• עבור על מדיניות והליכים • צפה במנגנוני הבקרה הפיזיים • צפה במאפייני האבטחה	☐	☐	☐	☐	☐
	ב. האם מצלמות האבטחה ו/או אמצעי בקרת הגישה האחרים מוגנים מפני חבלה או הפסקה של פעילותם?	• צפה בהליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ג. האם הנתונים שנאספו ממצלמות האבטחה או מאמצעי בקרת הגישה האחרים נבדקים ומושווים לנתונים מכניסות אחרות?, והאם הנתונים נשמרים למשך שלושה חודשים לפחות, אלא אם יש	• עבור על מדיניות והליכים • ראיין את עובדי האבטחה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	חוק מורה אחרת?						
	ד. האם הנתונים שנאספו ממצלמות האבטחה או מאמצעי בקרת הגישה האחרים נשמרים למשך שלושה חודשים לפחות, אלא אם יש חוק מורה אחרת?	• עבור על תהליכי שמירת המידע • צפה באחסון מידע • ראיין את עובדי האבטחה	☐	☐	☐	☐	☐
9.1.2	האם הגישה הפיזית לשקעי רשת שיש אליהם נגישות ציבורית מוגבלת? *לדוגמה, שקעי רשת לא יימצאו באזורים שיש בהם גישה לאורחים, אלא אם הגישה לרשת הותרה במפורש*. לחילופין, יש ליישם הליכים לוודא שיש תמיד ליווי של אורחים באזורים בהם יש חיבורי רשת פעילים.	• עבור על מדיניות והליכים • ראיין את כוח האדם • צפה במקומות	☐	☐	☐	☐	☐
9.1.3	האם הגישה הפיזית לנקודות גישה אלחוטיות, שערי תקשורת, מכשירים ניידים, חומרת רשת/תקשורת וקווי טלקומוניקציה מוגבלת?	• עבור על מדיניות והליכים • ראיין את כוח האדם • צפה במכשירים	☐	☐	☐	☐	☐
9.2	א. האם קיימים נהלים המאפשרים להבחין בקלות בין עובדי המקום למבקרים הכוללים: • זיהוי עובדים חדשים או אורחים (לדוגמה, מתן תגי זיהוי) • שינוי דרישות	• עבור על מדיניות והליכים • ראיין את כוח האדם • צפה בשיטות הזיהוי (כגון תגים) • צפה בהליכי אורחים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	גישה • ביטול זיהוי של אורחים שתוקפם פג או של עובדים שהפסיקו את עבודתם (כגון תגי זיהוי)? *לצרכי דרישה 9, "עובדי המקום" מתייחס לעובדים במשרה מלאה, עובדים במשרה חלקית, עובדים זמניים, קבלנים ויועצים שנוכחים פיזית בתוך מתחמי הארגון. "מבקר" מתייחס לספק, אורח של מי מעובדי המקום, או כל מי שצריך לבקר במתחם הארגון לפרק זמן קצר ובדרך כלל לא יותר מיום אחד.*						
	ב. האם התגים מזהים את המבקרים בצורה ברורה ועוזרים להבחין בקלות בין עובד למבקר? •	• צפה בשיטות זיהוי	☐	☐	☐	☐	☐
	ג. האם הגישה למערכת התגים מוגבלת לאנשים מורשים בלבד?	• צפה בבקרה פיזית ובקרות גישה למערכת התגים	☐	☐	☐	☐	☐
9.3	האם הגישה הפיזית לאזורים רגישים מוגבלת לעובדים בצורה הבאה: • האם הגישה מאושרת על בסיס צורכי התפקיד האישי? • האם הגישה מוגבלת מיידית עם פקיעת התוקף	• ראיין את כוח האדם • בחן רשימות בקרת גישה • צפה בעובדים במקום	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
• האם עובדים מתבקשים להחזיר את פריט הזיהוי הפיזי לפני שהם עוזבים את המתקן או כאשר תוקפו פג?		• השווה בין רשימות העובדים לשעבר לרשימות הבקרת גישה					
9.4	האם זיהוי ומתן גישה לאורחים נעשה כדלקמן:						
9.4.1	האם מבקרים מקבלים אישור כניסה טרם כניסתם לאזורים בהם נתוני כרטיסי אשראי מעובדים או מאוחסנים, ויש להם ליווי בכל זמן במשך הביקור?	• עבור על מדיניות והליכים • צפה בהליכים לאורחים, כולל בקרת הגישה • ראיין את כוח האדם • צפה באורחים ובשימוש בתג	☐	☐	☐	☐	☐
9.4.2	א. האם ניתן למבקרים פריט פיזי (למשל תג או אמצעי גישה) שמזהה אותם כאורחים?	• צפה בשימוש בתג של עובדים ואורחים • בחן זיהוי	☐	☐	☐	☐	☐
	ב. האם תוקף תגי המבקרים פוקע?	• צפה בהליך • בחן זיהוי	☐	☐	☐	☐	☐
9.4.3	האם מבקרים מתבקשים להחזיר את פריט הזיהוי הפיזי לפני שהם עוזבים את המתקן או כאשר תוקפו פג?	• צפה בתהליכים • צפה באורחים העוזבים את המקום	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
9.4.4	א. האם נעשה שימוש ביומן מבקרים המתעד גישה פיזית למתקן כמו גם לחדרי מחשב ומרכזי מידע בהם נתוני כרטיסי אשראי מאוחסנים או משודרים?	• עבור על מדיניות והליכים • בחן את יומן המבקרים • צפה בהליכים לאורחים • בחן את שמירת היומן	☐	☐	☐	☐	☐
	ב. האם יומן המבקרים מכיל את שם המבקר, החברה אותה הוא מייצג, ואת שם העובד אשר אישר את גישתו הפיזית,	• עבור על מדיניות והליכים • בחן את יומן המבקרים	☐	☐	☐	☐	☐
	ג. האם יומן המבקרים נשמר לפחות למשך שלושה חודשים?	• עבור על מדיניות והליכים • בחן את שמירת יומן המבקרים	☐	☐	☐	☐	☐
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	☐	☐	☐	☐	☐
9.5.1	א. האם מדיות הגיבוי מאוחסנות במקום מאובטח, רצוי באתר חיצוני כגון אתר גיבוי, אתר חלופי או מתקן	• צפה באבטחה הפיזית במקום אחסון	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	אחסון מסחרי?	המדיה					
	ב. האם האבטחה של המתקן נבדקת לפחות אחת לשנה?	• עבור על מדיניות והליכים לבדיקה של אתרים חיצוניים לאחסון מדיה • ראיין את עובדי האבטחה	☐	☐	☐	☐	☐
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	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		והתיעוד					
9.7	האם ישנה בקרה מחמירה על אופן האחסון והנגישות למדיות (המכילות נתוני כרטיסי אשראי)?	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
9.7.1	א. האם רשימות המלאי של המדיות מתוחזקות כראוי,	• בחן את רשימות המלאי	☐	☐	☐	☐	☐
	ב. האם מתבצע רישום מלאי לפחות אחת לשנה?	• בחן את רשימות המלאי • ראיין את כוח האדם	☐	☐	☐	☐	☐
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	☐	☐	☐	☐	☐
	ב. האם ההשמדה מתבצעת כדלהלן: • מדיה קשיחה נגרסת, נשרפת או נכתשת באופן שאינו מאפשר לשחזר את הנתונים של כרטיסי האשראי • מכלים המאחסנים מידע המיועד להשמדה מאובטחים • נתוני אשראי על גבי מדיה אלקטרונית מושמדים באמצעות תכנית השמדה מאובטחת (בהתאם לסטנדרטים המקובלים בתעשייה בנוגע למחיקה בטוחה), או לחילופין על ידי השמדה פיזית	• עבור על מדיניות והליכים להשמדת מדיה תקופתית	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	של המדיה.						
	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	☐	☐	☐	☐	☐
9.8.2	האם נתוני אשראי על גבי מדיה אלקטרונית מושמדים באמצעות תכנית השמדה מאובטחת, בהתאם לסטנדרטים המקובלים בתעשייה בנוגע למחיקה בטוחה, או לחילופין על ידי השמדה פיזית של המדיה(, כך שלא ניתן יהיה לשחזרם?	• צפה בתהליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
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, ולאחר מכן תהפוך לדרישה.*						
	א. האם המדיניות וההליכים מחייבים שמירת רשימה של	• עבור על מדיניות	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	מכשירים כאלו?	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 מיקום, יוצאים מכלל פעולה, ועוד?	• ראיין את כוח האדם	☐	☐	☐	☐	☐
9.9.2	א. האם משטחי המכשירים נבדקים תקופתית כדי לגלות התערבות (לדוגמה, הוספה של קוראי כרטיסים למכשיר) או	• ראיין את כוח האדם • צפה בהליכי הבדיקה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	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 חסרות או שונות, כיסוי שבור או בצבע שונה, או שינויים במספר הסידרתי או סימנים חיצוניים אחרים.*	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:						
	• 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 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	• עבור על חומר ההכשרה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	המתאימים (כגון מנהל או קצין אבטחה) על התנהגות חשודה וסימנים של התעסקות או החלפה של המכשיר.						
	• האם העובדים בנקודות המכירה קיבלו הכשרה, והם מודעים להליכים לגילוי ודיווח ניסיונות להתעסק עם המכשירים או להחליפם?	• ראיין עובדים בנקודות המכירה	☐	☐	☐	☐	☐
9.10	האם מדיניות אבטחה ונהלי הפעולה להצפנת תשדורות של נתוני מחזיקי כרטיסי אשראי: • מתועדים • בשימוש • ידועים לכל הצדדים הרלוונטיים?	• עבור על מדיניות האבטחה ונהלי הפעולה • ראיין את כוח האדם	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

בצע ניטור ובדיקה של הרשת באופן קבוע

דרישה 10: נטר ועקוב אחר כל גישה למשאבי הרשת ולנתוני כרטיסי האשראי

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
10.1	א. האם נתיב ביקורת מאופשר ופעיל עבור רכיבי המערכת?	• צפה בהליכים • ראיין מנהל מערכת	☐	☐	☐	☐	☐
	ב. האם הגישה לרכיבי המערכת קשורה למשתמשים מסוימים?	• צפה בהליכים • ראיין מנהל מערכת	☐	☐	☐	☐	☐
10.2	האם מיושם נתיב ביקורת אוטומטי (audit trails) עבור כל רכיבי המערכת על מנת שניתן יהיה לשחזר את האירועים הבאים:						
10.2.1	כל הגישות של משתמש יחיד לנתוני כרטיסי האשראי?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.2.2	כל הפעולות שבוצעו על ידי משתמש יחיד בעל הרשאות ניהול או הרשאות root?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.2.3	גישה לנתיב הביקורת (audit trails)?	• ראיין את כוח האדם • צפה ביומני	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		• הביקורת • בחן את הגדרות יומני הביקורת					
10.2.4	ניסיונות בלתי תקפים לקבלת גישה לוגית?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.2.5	שימוש במנגנוני הזיהוי והאימות - כולל אבל לא מוגבל ליצירת חשבונות חדשים והגברת הרשאות - וכל השינויים, התוספות או ההסרות לחשבונות עם הרשאות root ניהוליות?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.2.6	אתחול, עצירה או הפסקה של יומן הביקורת (audit log)?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.2.7	יצירה ומחיקה של אובייקט מערכת?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.3	האם השדות הבאים מופעים מופיעים בנתיב הביקורת (audit trail) של המערכת בעת התרחשות של						

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	כל אירוע (event) של המערכת?						
10.3.1	זהות המשתמש?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.3.2	סוג האירוע (event)?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.3.3	תאריך ושעה?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.3.4	סימון הצלחה או כישלון?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.3.5	מקור היווצרות האירוע?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		הגדרות יומני הביקורת					
10.3.6	זהותם או שמם של הנתונים, רכיבי המערכת או המשאבים המושפעים?	• ראיין את כוח האדם • צפה ביומני הביקורת • בחן את הגדרות יומני הביקורת	☐	☐	☐	☐	☐
10.4	א. האם כל שעוני וזמני המערכת מסונכרנים באמצעות שימוש בטכנולוגית סנכרון, והאם מקפידים על עדכון טכנולוגיה זו? ***הערה**: דוגמה אחת לטכנולוגית סנכרון היא פרוטוקול זמן רשת – Network time protocol (NTP).*	• עבור על סטנדרטים ותהליכים של קונפיגורציית הזמן	☐	☐	☐	☐	☐
10.4.1	האם הבקרות הבאות מיושמות עבור רכישה, הפצה ושמירה של ערכי זמן (תאריך ושעה):						
	א. האם רק שרתי זמן ייעודיים מקבלים אותות זמן ממקורות חיצוניים, והאם הזמן (תאריך ושעה) על כל המערכות הקריטיות הוא מדויק ועקבי בהתבסס על זמן בינלאומי אטומי (International Atomic Time) או UTC?	• עבור על סטנדרטים ותהליכים של קונפיגורציית הזמן • בחן פרמטרים של המערכת הקשורים בזמן	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
ב.	כאשר יש יותר משרת זמן ייעודי אחד, האם שרתי הזמן הייעודיים מתקשרים אחד עם השני על מנת לשמור על נכונות הזמן?	• עבור על סטנדרטים ותהליכים של קונפיגורציית הזמן • בחן פרמטרים של המערכת הקשורים בזמן	☐	☐	☐	☐	☐
ג.	האם השרתים הפנימיים מקבלים את הזמן רק משרתי הזמן המרכזיים?	• עבור על סטנדרטים ותהליכים של קונפיגורציית הזמן • בחן פרמטרים של המערכת הקשורים בזמן	☐	☐	☐	☐	☐
10.4.2	האם נתוני הזמן מוגנים באופן הבא:	• בחן את קונפיגורציית המערכת ואת הגדרות סינכרון הזמן	☐	☐	☐	☐	☐
א.	גישה לנתוני זמן מוגבלת רק לאנשים בעלי צורך עסקי לכך?						
ב.	שינויים בהגדרות הזמן של מערכות קריטיות, מתועדים, מנוטרים ונבדקים?	• בחן את קונפיגורציית המערכת ואת הגדרות ויומני סינכרון הזמן	☐	☐	☐	☐	☐
10.4.3	האם הגדרות הזמן מתקבלות ממקורות זמן ספציפיים המקובלים בתעשייה? (זאת על מנת למנוע מאדם זדוני לשנות את השעון). *ניתן לשקול את האפשרות להצפין את העדכונים הללו באמצעות מפתח סימטרי ולהכין רשימות בקרת גישה*	• בחן את קונפיגורציית המערכת	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	המפרטות את כתובת ה IP של המכונות שיקבלו את עדכוני הזמן (על מנת למנוע את השימוש האסור בשרתי זמן פנימיים).						
10.5	האם קבצי נתיבי הביקורת מאובטחים כך שלא ניתן יהיה לשנותם, באופן הבא:						
10.5.1	האם הרשאת הצפייה בקבצי נתיבי הביקורת מוגבלים לאלה שזקוקים לכך לצורך עבודתם?	• ראיין מנהלי מערכת • בחן את ההרשאות וקונפיגורציי ת המערכת	☐	☐	☐	☐	☐
10.5.2	האם קבצי נתיבי הביקורת מוגנים מפני שינויים בלתי מורשים באמצעות אמצעי בקרת גישה, הפרדה פיזית ו/או הפרדת רשתות?	• ראיין מנהלי מערכת • בחן את ההרשאות וקונפיגורציי ת המערכת	☐	☐	☐	☐	☐
10.5.3	האם קבצי נתיבי הביקורת מגובים מידית לשרת לוג (log) מרכזי או למדיה שקשה לעשות בה שינויים?	• ראיין מנהלי מערכת • בחן את ההרשאות וקונפיגורציי ת המערכת	☐	☐	☐	☐	☐
10.5.4	האם לוגים של טכנולוגיות הפונות החוצה (כגון: wireless, firewalls, DNS, ו mail), מורדים או מועתקים לשרת לוג מרכזי מאובטח או למדיה ברשת הפנימית?	• ראיין מנהלי מערכת • בחן את ההרשאות וקונפיגורציי ת המערכת	☐	☐	☐	☐	☐
10.5.5	האם נעשה שימוש בתוכנות לבדיקת שלמות קבצים או זיהוי שינויים על קבצי הלוג, על מנת להבטיח שלא ניתן יהיה לשנות את המידע הקיים בקובץ הלוג ללא שתיוצר התראה המתריעה	• בחן הגדרות, קבצים מנוטרים ותוצאות מפעילויות מנוטרות	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	על כך (למרות שמידע חדש שמתוסף ללוג לא צריך לייצר התראה)?						
10.6	האם הלוג היומנים וכל אירועי האבטחה של כל רכיבי המערכת נסקרים חריגים כדי לזהות פעילות חריגה או חשודה כדלקמן:? *__הערה__: ניתן להשתמש בטכנולוגיות כגון כלי איסוף, ניתוח והתראה של לוגים על מנת לעמוד בדרישה 10.6*						
10.6.1	א. האם המדיניות וההליכים הכתובים מגדירים שיש לעבור על היומנים והאירועים לפחות פעם ביום, באופן ידני או דרך כלי היומן? • כל אירועי האבטחה • יומנים של כל רכיבי המערכת המאחסנים, מעבדים או משדרים CHD ו/או SAD, או שיכולים להשפיע על האבטחה של CHD ו/או SAD • יומנים של כל רכיבי מערכת קריטיים • יומנים של כל השרתים ורכיבי המערכת המבצעים תפקודי אבטחה (כגון firewall, מערכות לגילוי חדירה/ מערכות למניעת חדירה	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	(IDS/IPS), שרתי אימות, שרתי ניתוב מחדש של מסחר אלקטרוני ועוד)						
	ב. האם היומנים ואירועי האבטחה לעיל מבוקרים לפחות פעם ביום?	• צפה בהליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
10.6.2	א. האם המדיניות וההליכים הכתובים מגדירים שיש לעבור על היומנים או כל רכיבי המערכת האחרים באופן קבוע, באופן ידני או דרך כלי היומן, בהתבסס על אסטרטגיית ניהול הסיכונים והמדיניות של הארגון?	• עבור על מדיניות והליכי האבטחה	☐	☐	☐	☐	☐
	ב. האם סקירות של כל מרכיבי המערכת האחרים מבוצעות בהתאם לאסטרטגיית ניהול הסיכונים והמדיניות של הארגון?	• עבור על מסמכי ניהול סיכון • ראיין את כוח האדם	☐	☐	☐	☐	☐
10.6.3	א. האם מדיניות ותהליכים כתובים מגדירים מעקב אחר חריגים ויוצאי דופן שזוהו בהליך הביקורת?	• עבור על מדיניות והליכי האבטחה	☐	☐	☐	☐	☐
	ב. האם בוצע מעקב אחר חריגים ויוצאי-דופן?	• צפה בהליכים • ראיין את כוח האדם	☐	☐	☐	☐	☐
10.7	א. האם קיימים נהלי	• עבור על	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	שימור של קבצי לוג ביקורת (audit logs), והאם הם כוללים דרישה שההיסטוריה של נתיבי הביקורת תישמר למשך שנה לפחות, כשלפחות שלושה חודשים יהיו זמינים לניתוח מיידי (לדוגמה, אחסון מקוון, בארכיב, או ניתן לשחזור מעותק גיבוי)?	מדיניות והליכים של האבטחה					
ב.	האם קבצי לוג ביקורת (audit logs) זמינים למשך שנה לפחות?	• ראיין את כוח האדם • בחן יומני ביקורת	☐	☐	☐	☐	☐
ג.	האם הלוגים של שלושת החודשים האחרונים לפחות זמינים מיידית לצרכי ניתוח?	• ראיין את כוח האדם • צפה בהליכים	☐	☐	☐	☐	☐
10.8	האם מדיניות אבטחה ונהלי הפעולה להצפנת תשדורות של נתוני מחזיקי כרטיסי אשראי: • מתועדים • בשימוש • ידועים לכל הצדדים הרלוונטיים?	• עבור על מדיניות האבטחה ונהלי הפעולה • ראיין את כוח האדם	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

דרישה 11: בצע בדיקות שוטפות של מערכות ותהליכי האבטחה

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
11.1	א. האם יש תהליכים מיושמים לגילוי וזיהוי של נקודות גישה אלחוטיות מורשות ובלתי מורשות על בסיס רבעוני? ***הערה**: השיטות שבהן ניתן לעשות שימוש בתהליך זה כוללות, אך אינן מוגבלות לאמצעים הבאים: סריקה של רשתות אלחוטיות, בדיקות פיזיות/לוגיות של רכיבי מערכת ותשתית, בקרת גישת רשת (NAC) או פריסת IDS/IPS אלחוטי.* *יהיו אשר יהיו השיטות שבהן נעשה שימוש, עליהן להיות מספיקות לאיתור וזיהוי של כל התקן בלתי מורשה.*	• עבור על מדיניות והליכים	☐	☐	☐	☐	☐
	ב. האם השיטה לגילוי וזיהוי של נקודות גישה אלחוטיות לא מורשות כוללת גילוי וזיהוי של הרכיבים הבאים לכל הפחות: • כרטיס רשת אלחוטית (WLAN) שהוכנסו לרכיבי מערכת; • מכשירים אלחוטיים ניידים שחוברו לרכיבי מערכת כדי ליצור נקודת גישה אלחוטית (למשל, באמצעות USB,	• הערך את השיטה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	וכו) ; • מכשיר אלחוטי המחובר לערוץ (port) רשת או למכשיר ברשת?						
	ג. האם התהליך לזיהוי נקודות גישה אלחוטיות מורשות ובלתי מורשות מבוצע על כל רכיבי המערכת והמתקנים בכל האתרים ולפחות פעם ברבעון?	• בחן פלט מסקירות אלחוטיות אחרונות	☐	☐	☐	☐	☐
	ד. האם מיושם ניטור אוטומטי (למשל, IPS/IDS אלחוטי, NAC, וכו'), האם הניטור מוגדר לייצר התראות לעובדים?	• בחן הגדרות קונפיגורציה	☐	☐	☐	☐	☐
11.1.1	האם יש מלאי של נקודות גישה אלחוטית מורשות עם תיעוד של סיבות עסקיות עבור כל נקודות הגישה האלחוטית המורשות? ?	• בחן רשומות מלאי	☐	☐	☐	☐	☐
11.1.2	א. האם התוכנית לתגובה לאירוע מגדירה ומצריכה תגובה במקרה ונמצאה נקודת גישה אלחוטית בלתי מורשת?	• בחן תוכנית תגובה לאירוע (ראה דרישה 12.10)	☐	☐	☐	☐	☐
	ב. האם ננקטת פעולה כאשר מתגלית נקודת גישה אלחוטית בלתי מורשית?	• ראיין את העובדים האחראים • בדוק סקירות אלחוטיות אחרונות ותגובות קשורות	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
11.2	האם סריקות פנימיות וחיצוניות לאיתור פרצות רשת מורצות לפחות אחת לרבעון ולאחר כל שינוי משמעותי ברשת (התקנת רכיבי מערכת חדשים, שינויים בטופולוגית הרשת, שינויים בחוקי ה-firewall שדרוגים של מוצרים) באופן הבא? ***הערה**: אפשר לאחד דוחות סקירה מרובים עבור הליך הסקירה הרבעוני כדי להראות שכל המערכות נסרקו וכל נקודות התורפה הרלוונטיות טופלו. ייתכן וידרשו מסמכים נוספים כדי לוודא שיגיעו גם לנקודות תורפה שלא טופלו* *אין חובה שארבע סריקות רבעוניות עם תוצאה עוברת יושלמו לקראת תאימות <u>ראשונית</u> עם תקן PCI DSS אם 1) הסריקה האחרונה היתה בעלת תוצאה עוברת, 2) הישות תעדה מדיניות ונהלים הדורשים סריקה רבעונית, ו 3) נקודות התורפה שנמצאו בסריקה ומופיעות בדוח הסריקה תוקנו כפי שמוכיחה סריקה החוזרת. עבור תאימות לתקן בשנים שאחרי הסקירה הראשונית של PCI, יש חובה לבצע 4 סריקות רבעוניות עם תוצאה עוברת.*						
11.2.1	א. האם מתבצעות סריקות פנימיות למציאת נקודות תורפה אחת לרבעון?	• עבור על דוחות סקירה	☐	☐	☐	☐	☐
	ב. האם תהליך הסריקה הפנימית הרבעוני כולל סריקות חוזרות עד אשר מתקבלת תוצאה עוברת או עד אשר כל נקודות התורפה המדורגות	• עבור על דוחות סקירה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	ברמת סיכון "גבוהה" כמוגדר בדרישה 6.1 של PCI DSS, טופלו?						
	ג. האם הסריקות הפנימיות הרבעוניות מבוצעות על ידי כח אדם פנימי או חיצוני מיומן, וכאשר רלוונטי, האם מתקיים עקרון אי התלות של הבודק בארגון (לא חייב להיות QSA או ASV)?	• עבור על דוחות סקירה	☐	☐	☐	☐	☐
11.2.2	א. האם מבוצעות סריקות רבעוניות חיצוניות למציאת נקודות תורפה? ***הערה:*** *סקירות חיצוניות רבעוניות חייבות להיות מבוצעות על ידי ספק סקירה מאושר (ASV) המאושר על ידי ה- PCI SSC.* *ראה במדריך ה-ASV המפורסם באתר PCI SSC עבור אחריות הלקוח לסריקה, הכנות לסריקה ועוד*	• עבור על התוצאות מארבעת הרבעונים האחרונים של סקירה חיצונית למציאת נקודות תורפה	☐	☐	☐	☐	☐
	ב. האם הסריקות החיצוניות הרבעוניות מקיימות את דרישות תכנית ההדרכה של ASV (למשל, לא צריכות להימצא בסריקה נקודות תורפה המדורגות גבוה יותר מ 4.0 על פי דירוג ה CVSS ולא כישלונות	• עבור על התוצאות של כל סקירה רבעונית חיצונית וסקירה מחדש	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	אוטומטיים)?						
	ג. האם הסריקות הרבעוניות החיצוניות מבוצעות על ידי ספק סריקה מאושר (ASV), אשר אושר על ידי מועצת ה PCI (PCI SSC)?	• עבור על התוצאות של כל סקירה רבעונית חיצונית וסקירה מחדש	☐	☐	☐	☐	☐
11.2.3	א. האם סריקות פנימיות וחיצוניות וסריקות מחדש מבוצעות לאחר כל שינוי מהותי? ***הערה**: הסריקות חייבות להתבצע על ידי כח אדם מיומן.*	• בחן ותאם מסמכים על בקרת שינויים ודוחות סקירה	☐	☐	☐	☐	☐
	ב. האם תהליך הסריקה כולל סריקות חוזרות עד אשר: • עבור סריקות חיצוניות – אין נקודות תורפה קיימות אשר קיבלו ציון גבוה מ 4.0 על פי דירוג ה CVSS • עבור סריקות פנימיות – התקבלה תוצאה עוברת או לחילופין כל נקודות התורפה המדורגות ברמת סיכון	• עבור על דוחות הסקירה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
"גבוהה" טופלו בהתאם למוגדר בדרישה 6.1 ל PCI DSS.						
ג. האם הסריקות מבוצעות על ידי כח אדם פנימי או חיצוני מיומן, וכאשר רלוונטי, האם מתקיים עקרון אי התלות של הבודק בארגון (לא חייב להיות QSA או ASV)?	• ראיין את כוח האדם	☐	☐	☐	☐	☐
11.3 האם המתודולוגיה של בדיקת החדירות כוללת את האלמנטים הבאים: • מבוססת על שיטות בדיקה מקובלות בתעשייה (למשל NIST SP800-15) • מכסה את כל סביבת התשלום בארגון ואת המערכות הקריטיות של הארגון. • נעשית גם מתוך וגם מחוץ לרשת הארגונית. • בדיקות שנועדו לוודא את יעילות הבקרות שהושמו על מנת להפריד את סביבת התשלום מיתר הארגון ו/או וידוא של בקרות שהושמו על מנת להקטין את היקף התכולה של התקן בו הארגון נדרש לעמוד. • רשימת בדיקות	• ראיין את כוח האדם • בחן תהליך בדיקות חדירה					

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	חדירות ברמת האפליקציה הכוללת לכל הפחות את רשימות נקודות התורפה המנויות בסעיף 6.5 • רשימת בדיקות חדירות הרמת הרשת המכסות גם אלמנטים התומכים בפעילות הרשת ואת מערכות ההפעלה. • מעבר ובחינה של איומים ונקודות תורפה שהתגלו בארגון במהלך 12 החודשים הבאים. • הגדרה של תקופת השמירה של תוצאות הבדיקה ושל תוצאות הפעילות המתקנת בעקבות הבדיקה.						
11.3.1	א. האם מתבצעת בדיקת חדירות (penetration testing) *חיצונית* לפי השיטה המוגדרת לפחות פעם בשנה או אחרי כל שינוי מהותי בתשתיות או באפליקציות (כגון, עדכון מערכת ההפעלה, הוספת רשת משנה לסביבה, או הוספת שרת web לסביבה)?	• בחן את היקף העבודה • בחן את התוצאות ממבחן החדירה החיצוני האחרון	☐	☐	☐	☐	☐
	ב. האם הבדיקות מבוצעות על ידי כח אדם פנימי או חיצוני מיומן, וכאשר רלוונטי, האם מתקיים עקרון אי	• בחן את היקף העבודה • ראיין את העובדים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	התלות של הבודק בארגון (לא חייב להיות QSA או ASV)?	האחראים					
11.3.2	א. האם מתבצעת בדיקת חדירות (penetration testing) *פנימית* לפי השיטה המוגדרת לפחות פעם בשנה או אחרי כל שינוי מהותי בתשתיות או באפליקציות (כגון, עדכון מערכת ההפעלה, הוסספת רשת משנה לסביבה, או הוספת שרת web לסביבה)?	• בחן את היקף העבודה • בחן את התוצאות ממבחן החדירה החיצוני האחרון	☐	☐	☐	☐	☐
	ב. האם הבדיקות מבוצעות על ידי כח אדם פנימי או חיצוני מיומן, וכאשר רלוונטי, האם מתקיים עקרון אי התלות של הבודק בארגון (לא חייב להיות QSA או ASV)?	• בחן את היקף העבודה • ראיין את העובדים האחראים	☐	☐	☐	☐	☐
11.3.3	האם נקודות תורפה שנמצאו כניתנות לניצול, תוקנו ולאחר מכן בוצעה בדיקה חוזרת?	• בחן את תוצאות בדיקת החדירה					
11.3.4	אם יש שימוש בסגמנטציה כדי לבודד את ה-CDE מרשתות אחרות: א. האם תהליכים לבדיקת חדירות מוגדרים לבדיקת כל שיטות הסגמנטציה, לאשר שהן פעילות ויעילות ולבודד את כל המערכות שמחוץ להיקף מהמערכות	• בחן בקרת סגמנטציה • עבור על שיטת בדיקת חדירות					

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	שבהיקף?						
	ב. האם בדיקות החדירה לוודא ביקורת סגמנטציה עונות על התנאים הבאים: • מבוצעות לפחות פעם בשנה ולאחר שינויים בשיטת/ בקרת הסגמנטציה • מכסות את כל שיטות/ בקרת הסגמנטציה שבשימוש • מוודאות ששיטות הסגמנטציה פעילות ויעילות ומבודדות את כל המערכות שמחוץ להיקף מהמערכות שבהיקף	• בחן תוצאות מבדיקת החדירה האחרונה	☐	☐	☐	☐	☐
11.4	א. האם נעשה שימוש במערכות זיהוי חדירה (IDS) ו/או מערכות מניעת חדירה (IPS) כדי לנטר את כל התעבורה?	• בחן את קונפיגורציי ת המערכת • בחן את דיאגרמות הרשת	☐	☐	☐	☐	☐
	ב. האם מערכות ה IPS/IDS הוגדרו לשלוח התראות לגורמים הרלוונטיים כאשר יש חשד לפעילות זדונית?	• בחן את קונפיגורציי ת המערכת • ראיין את כוח האדם	☐	☐	☐	☐	☐
	ג. האם מקפידים על עדכון של כל רמות הבסיס (base	• בחן את קונפיגורציי	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	line),המנועים והחתימות של מערכות ה IDS/IPS ?	• בחן את מסמכי הספקים ת IPS/IDS	☐	☐	☐	☐	☐
11.5	א. האם מיושם מנגנון לגילוי שינוי (לדוגמה כלים לניטור שלמות קבצים (file integrity)) בסביבת נתוני כרטיסי האשראי כדי לגלות שינויים בלתי מורשים בקבצי מערכת חיוניים, קבצי קונפיגורציה, או קבצי תוכן? *דוגמאות לסוגי קבצים שצריכים להיות מנוטרים:* • *קבצי מערכת הניתנים להרצה (executables)* • *קבצי אפליקציה הניתנים להרצה (executables)* • *קבצי פרמטרים וקבצי קונפיגורציה* • *קבצי לוג וביקורת הנשמרים בצורה מרוכזת, בהיסטוריה או בארכיב* • *קבצים חיוניים נוספים הנקבעים על ידי אחראי (כגון דרך הערכת סיכונים או בדרכים נוספות)*	• צפה בהגדרות המערכת וקבצים מנוטרים • בחן את הגדרות קונפיגורציי ת המערכת	☐	☐	☐	☐	☐
	ב. האם הכלים	• צפה	☐	☐	☐	☐	☐

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	מוגדרים לשלוח התרעות לגורמים הרלוונטיים על כל שינוי לא מורשה של קבצי מערכת קריטיים, קבצי קונפיגורציה או קבצי תוכן, והאם הכלים מבצעים השוואות קבצים קריטיים לפחות פעם בשבוע? ***הערה**: לצורך ניטור שלמות הקבצים – קבצים קריטיים הם אלו שבדרך כלל אינם עוברים שינויים תכופים, אך שינויים בהם עשויים להצביע על פגיעה במערכת או חשש לפגיעה. כלי ניטור שלמות קבצים מגיעים בדרך כלל עם הגדרות מוכנות מראש עבור קבצים קריטיים במערכת ההפעלה הרלוונטית. קבצים קריטיים אחרים, כגון קבצים לאפליקציות שפותחו פנימית, צריכים לעבור הערכה והגדרה על ידי הישות (כלומר בית העסק או ספק השירות).*	• עבור על התוצאות מפעילות הניטור בהגדרות המערכת וקבצים מנוטרים					
11.5.1	האם יש תהליך להגבה על התראות המיוצרות על ידי פתרון גילוי שינוי?	• בחן את הגדרות קונפיגורציי ת המערכת					
11.6	האם מדיניות אבטחה ונהלי הפעולה לניטור ובדיקות אבטחה: • מתועדים • בשימוש • ידועים לכל הצדדים הרלוונטיים?	• עבור על מדיניות האבטחה ונהלי הפעולה • ראיין את כוח האדם	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

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	☐	☐	☐	☐	☐
12.2	א. האם ישנו תהליך מתועד של הערכת סיכונים שנתית אשר מזהה סכנות ונקודות תורפה? *(דוגמאות למתודולוגיות הערכת סיכונים כוללות אבל לא מוגבלות ל: OCTAVE, ISO27005 ו- NIST SP 800-30).*	▪ עבור על תהליך הערכת הסיכון ▪ ראיין את כוח האדם	☐	☐	☐	☐	☐
	ב. האם תהליך הערכת הסיכון מסתיים בהערכת סיכון רשמית?	▪ עבור על הערכת הסיכון הרשמית					
	ג. האם הליך הערכת הסיכון מתבצע לפחות פעם בשנה ולאחר שינויים משמעותיים בסביבה (כגון מיזוג, רכישה, מעבר מקום ועוד)?	▪ עבור על המסמכים של הערכת הסיכון ▪ ראיין עובדים					

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		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	☐	☐	☐	☐	☐
12.3.2	אימות המשתמש עבור השימוש בטכנולוגיה?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.3	רשימה של המכשירים מסוג זה והעובדים בעלי הגישה?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.4	תיוג המכשירים לזיהוי הבעלים, פרטי ההתקשרות וייעוד המכשיר?	▪ עקוב אחר מדיניות שימוש ▪ ראיין	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		מדגם של עובדים אחראיים					
12.3.5	שימושים מקובלים בטכנולוגיה?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.6	מיקומי רשת מקובלים עבור הטכנולוגיות?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.7	רשימת המוצרים המאושרים לשימוש על ידי החברה?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.8	ניתוק אוטומטי של חיבורי גישה מרחוק לאחר פרק זמן מוגדר של חוסר פעילות?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
12.3.9	הפעלת טכנולוגיות גישה מרחוק עבור יצרנים ושותפים עסקיים רק כשהיצרנים והשותפים העסקיים זקוקים לגישה כזאת וסגירתה מיד בתום השימוש?	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		עובדים אחראיים					
12.3.10	א. האם המדיניות מציינת עבור אנשים המתחברים לסביבת נתוני כרטיסי האשראי כי חל איסור להעתיק, להעביר או לאחסן נתוני כרטיסי אשראי על דיסקים קשיחים מקומיים ועל מדיות אלקטרוניות נשלפות, אלא אם ניתן לכך אישור מפורש על מנת לענות על צורך עסקי מוגדר? *כאשר יש צורך עסקי מאושר, מדיניות השימוש מחייבת שהנתונים יהיו מוגנים בהתאם לכל דרישות PCI DSS הרלוונטיות.*	▪ עקוב אחר מדיניות שימוש ▪ ראיין מדגם של עובדים אחראיים	☐	☐	☐	☐	☐
	ב. 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	א. האם האחריות הרשמית לנושא אבטחת המידע מוטלת באופן רשמי על קצין אבטחת מידע או על	▪ עבור על מדיניות והליכים של אבטחת	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	גורם אחר בהנהלה בעל ידע מקצועי בתחום אבטחת מידע?	מידע					
	ב. האם סמכויות הניהול הבאות בתחום אבטחת המידע מוקצות לאדם או לקבוצה:						
12.5.1	פיתוח, תיעוד והפצת מדיניות ונהלי אבטחת מידע?	▪ עבור על מדיניות והליכים של אבטחת מידע	☐	☐	☐	☐	☐
12.5.2	ניטור וניתוח התרעות ומידע אבטחה, והפצתם לסגל האנשים המתאים?	▪ עבור על מדיניות והליכים של אבטחת מידע	☐	☐	☐	☐	☐
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	☐	☐	☐	☐	☐
12.5.4	ניהול חשבונות משתמש לרבות הוספות, מחיקות ועדכונים?	▪ עבור על מדיניות והליכים של אבטחת מידע	☐	☐	☐	☐	☐
12.5.5	ניטור ובקרה על כל גישה למידע?	▪ עבור על מדיניות והליכים של אבטחת מידע	☐	☐	☐	☐	☐
12.6	א. האם ישנה תכנית מודעות אבטחה רשמית שתפקידה לגרום לכלל העובדים	▪ עבור על התוכנית למודעות לאבטחה	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	להיות מודעים לחשיבות אבטחת נתוני כרטיסי אשראי?						
	ב. האם נהלי תכנית המודעות לאבטחה כוללת את הדברים הבאים:						
12.6.1	א. האם התוכנית מציעה מספר דרכים לחנך ולהגביר את המודעות בקרב העובדים (לדוגמה, פוסטרים, מכתבים, הכשרה ברשת (web based training), פגישות)? **הערה**: שיטות ההדרכה עשויות להשתנות בכפוף לתפקידו של העובד ולרמת הגישה שלו לנתונים.	▪ עבור על תוכנית מודעות לאבטחה ▪ עבור על התהליכים של התוכנית למודעות לאבטחה ▪ עבור על רשימות הנוכחות של התוכנית למודעות לאבטחה	☐	☐	☐	☐	☐
	ב. האם העובדים מקבלים את הדרכה מיד עם קבלתם לעבודה ולפחות פעם בשנה?	▪ בחן את נהלי ותיעוד התוכנית למודעות לאבטחה	☐	☐	☐	☐	☐
	ג. האם עובדים השלימו הכשרה למודעות והאם הם מודעים לחשיבות אבטחת נתוני כרטיסי אשראי?	▪ ראיין את כוח האדם					
12.6.2	האם העובדים נדרשים לאשר לפחות פעם בשנה כי הם קראו והם מבינים את מדיניות ונהלי אבטחת המידע?	▪ בחן את נהלי ותיעוד התוכנית למודעות לאבטחה	☐	☐	☐	☐	☐
12.7	האם אנשים המועמדים	▪ ראיין את	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	להצטרף לכח האדם של החברה (ראה הגדרת "כח אדם" לעיל) עוברים סינון לפני העסקתם על מנת למזער את הסיכון להתקפות ממקורות פנימיים? *דוגמאות של בדיקת רקע כוללות רקע תעסוקתי קודם, רישום פלילי, היסטוריית אשראי ובדיקת המלצות.* ***הערה:** עבור עובדים פוטנציאליים המועסקים במשרות מסוימות, כגון קופאים, המספקות להם גישה למספר כרטיס אשראי אחד בכל פעם, בעת ביצוע עסקה, דרישה זו היא בבחינת המלצה בלבד.*	הנהלת מחלקת משאבי אנוש					
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*	▪ צפה בהסכמים הכתובים ▪ עבור על מדיניות והליכים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	המדויק המופיע בדרישה זו.						
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 ומסמכים תומכים	☐	☐	☐	☐	☐
12.9	*דרישה זו רלוונטית רק לספקי שירות.*		☐	☐	☐	☐	☐
12.10	האם מיושמת תכנית תגובה לאירוע אבטחה למקרה שבו יהיה צורך להגיב באופן מידי לאירוע של פריצת אבטחה במערכת, כדלקמן:						
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	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה	בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
		כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
	לאירוע					
ב. האם התכנית כוללת לכל הפחות:						
▪ הקצאת תפקידים, תחומי אחריות, ואסטרטגיות תקשורת ויצירת קשר במקרה של סכנת אבטחה כולל עדכון חברות האשראי, לכל הפחות?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
▪ נהלי תגובה מוגדרים וספציפיים לאירועי אבטחה?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
▪ נהלי התאוששות והמשכיות עסקית?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
▪ תהליכי גיבוי מידע?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
▪ ניתוח דרישות החוק בנוגע לדיווח על אירועי פרצות אבטחה?	▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
▪ כיסוי ותגובה	▪ עבור על	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
בנוגע לכל רכיבי המערכת הקריטיים?		התהליכים לתוכנית תגובה לאירוע					
▪ הפנייה או והטמעה של נהלי התגובה של חברות המותג של כרטיסי האשראי לאירועי אבטחה?		▪ עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
12.10.2	האם התכנית נבדקת לפחות פעם בשנה?	• עבור על התהליכים לתוכנית תגובה לאירוע • ראיין את העובדים האחראים	☐	☐	☐	☐	☐
12.10.3	האם מונו אנשים ספציפיים להיות זמינים למשך 24 שעות ביום 7 ימים בשבוע על מנת לתת מענה להתראות?	• צפה בהליכים • עבור על הנהלים • ראיין את העובדים האחראים	☐	☐	☐	☐	☐
12.10.4	האם ניתנת הכשרה נאותה לצוות האחראי לתת מענה לאירועי אבטחה?	• צפה בהליכים • עבור על התהליכים לתוכנית תגובה לאירוע • ראיין את העובדים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

שאלה		בדיקות נדרשות	תגובה (סמן תגובה אחת לכל שאלה)				
			כן	כן עם CCW	לא	לא רלוונטי	לא נבדק
		האחראים					
1210.5	האם תכנית תגובה לאירוע אבטחה כוללת קבלת התראות ממערכות IPS /IDS ומערכות לניטור שלמותם של קבצים?	• צפה בהליכים • עבור על התהליכים לתוכנית תגובה לאירוע	☐	☐	☐	☐	☐
12.10.6	האם פותח ומיושם תהליך לעדכון ופיתוח תכנית התגובה לאירוע אבטחה, בהתאם ללקחים שנלמדו ובהתאם להתפתחויות בתעשייה?	• צפה בהליכים • עבור על התהליכים לתוכנית תגובה לאירוע • ראיין את העובדים האחראים	☐	☐	☐	☐	☐

Copyright 2014 PCI Security Standards Council LLC

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

נספח זה אינו לשימוש הערכת בתי עסק.

Copyright 2014 PCI Security Standards Council LLC

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.	

Copyright 2014 PCI Security Standards Council LLC

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.*

Copyright 2010 PCI Security Standards Council LLC

נספח ד': הסבר על דרישות שלא נבחנו (Not Tested)

אם נעשה שימוש בעמודת "לא נבחן" בשאלון הערכה עצמית, יש להשתמש בגיליון עבודה זה כדי להסביר מדוע הדרישה לא נבחנה כחלק משאלון ההערכה.

דרישה	תאר איזה חלק (ים) של הדרישה לא נבחן	תאר מדוע הדרישות לא נבחנו
דוגמא: דרישה 12	*דרישה 12.2 הייתה הדרישה היחידה שנבדקה. כל יתר הדרישות האחרות מדרישה 12 לא נבחנו.*	*הערכה זו מכסה רק דרישות מאבן דרך 1 במסמך גישת התעדופים (Prioritized Approach).*
דוגמא: דרישה 1-8, 10-12	*רק דרישה 9 נבחנה בשאלון ההערכה. כל יתר הדרישות לא נבחנו.*	*החברה הינה ספק אירוח פיזי (CO-LO), ובקרות אבטחה פיזיות בלבד נבחנו לצורך ההערכה זו.*

Copyright 2014 PCI Security Standards Council LLC

פרק 3 – אישור ואימות פרטים

חלק 3. אישור PCI DSS

בהסתמך על התוצאות שהתקבלו בשאלון D 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 מותגי(ן) 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 D 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.
☐	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.

Copyright 2014 PCI Security Standards Council LLC

☐	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.

Copyright 2014 PCI Security Standards Council LLC

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) 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.	☐	☐	
8	זהה ואשר גישה לרכיבי מערכת.	☐	☐	
9	הגבל את הגישה הפיזית לנתונים של כרטיסי האשראי.	☐	☐	
10	נטר ועקוב אחר כל גישה למשאבי הרשת ולנתוני כרטיסי האשראי.	☐	☐	
11	בצע בדיקות שוטפות של מערכות ותהליכי האבטחה.	☐	☐	
12	יישם ותחזק מדיניות המטפלת באבטחת מידע בקרב כלל כח האדם (עובדים וקבלנים).	☐	☐	

Copyright 2014 PCI Security Standards Council LLC