נציג בית עסק נכבד,

שאלון ההערכה העצמית SAQ A תורגם מהשפה האנגלית לשפה העברית על מנת לסייע לך בהבנת דרישות התקן הרלוונטיות.

יודגש כי השאלון המקורי נכתב בשפה האנגלית והוא הנוסח המחייב.

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

למרות כל המאמצים והזהירות בתרגום השאלון מהשפה האנגלית , חברת לאומי קארד בע"מ, אינה ערבה לטיב התרגום ו/או דיוקו.

לכן חברת לאומי קארד בע "מ לא תישא בכל אחריות ו /או נזק עקב השימוש בשאלון בשפה העברית.

מודגש בזאת כי הנעזר בשאלון המתורגם בשפה העברית עושה זאת על דעתו ועל אחריותו בלבד.

לנוחיותך השאלון מולא מראש על ידי לאומי קארד על מנת להקל עליך בהליך ההערכה.

יחד עם זאת, הנך נדרש לעבור בעיון על השאלון והתשובות לו ולוודא כי האמור בשאלון הינו נכון, מדויק ומלא ולאשר זאת בחתימתך בתחתית השאלון.

לאומי קארד לא תישא בכל אחריות ו /או נזק עקב תשובות לשאלון שאינן נכונות, מדויקות ומלאות.

בברכה,

לאומי קארד

דף הוראות והסבר למילוי שאלון הערכה עצמית-A

מסמך השאלון מחולק לשלושה חלקים:

<u>הצהרת עמידה בתקן</u>

שים לב- למרות שחלק זה מופיע ראשון במסמך השאלון יש למלא אותו רק בסוף מילוי השאלון עצמו. לא ניתן להצהיר על עמידה או על אי עמידה בתקן ללא מילוי השאלון קודם.

א. חלק 1 א – "שם החברה"- לרשום את השם המשפטי של החברה. "שם מסחרי"- לרשום את שם החברה שידוע לציבור.

ב. חלק 2 - לסמן V בריבוע הרלוונטי.אם אין ריבוע רלוונטי נא לסמן V בריבוע "אחר" ולפרט את הפעילות של חברתך. בשדה "נא לציין מתקנים ואתרים הנכללים בסקר PCI DSS זה" יש לרשום את ה-URL של האתר שלך.

ג. חלק 2 א – בשאלה הראשונה יש לסמן V בריבוע "כן". בשאלה השנייה יש לסמן V בריבוע "כן" רק אם חברתך סולקת עם עוד סולק זולת חברת לאומי קארד.

ד. חלק 2 ב – אם כל הסעיפים בחלק זה אכן נכונים יש לסמן V <u>בכולם</u>.

ה. חלק 3 - שים לב! יש למלא את כל השדות אשר צבועות באפור בין סוגריים.אתה רשאי לסמן V בריבוע של "עומד בתקן" **<u>רק</u>** אם סימנת V בטורים "כן" או "אחר" **בכל** השאלות. אם סימנת V בטור "לא" לאחת או יותר מהשאלות בשאלון יש לסמן V בריבוע "לא עומד בתקן".

ו. חלק 3 א – אם כל הסעיפים בחלק זה אכן נכונים יש לסמן V <u>בכולם</u>. בסעיף הראשון יש לרשום **2.0** בן הסוגריים שמופיעים (מס' הגרסה של השאלון)

ז. חלק 3 ב- שים לב! **ללא מילוי חלק זה <u>כולל חתימה</u> אין תוקף לשאלון.**

<u>השאלון עצמו</u>

א. שים לב! יש למלא את התאריך בשדה האפור בראש העמוד בצד ימין- "תאריך מילוי הטופס"

ב. ליד כל שאלה תמצא שלושה טורים כתשובה אפשרית – "כן"/"לא"/"אחר"

ג. אם השאלה רלוונטית עבורך ואתה עומד בדרישה יש לסמן V בטור "כן"

ד. אם השאלה רלוונטית עבורך אך אינך עומד בדרישה יש לסמן V בטור "לא"

ה. אם השאלה לא רלוונטית עבורך יש לסמן V בטור "אחר".יש לנמק מדוע היא לא רלוונטית בנספח D בסוף השאלון (ראה מטה).

ו. יש לענות על כל השאלות בשאלון. אין להשאיר שאלה ללא סימון באחד הטורים "כן"/"לא"/"אחר"

<u>נספחים</u>

א. נספח ד- אם רשמת V בטור "אחר" לאחת או יותר מהשאלות בשאלון , עליך לפרט את הסיבה לכך.יש לרשום את מספר הסעיף הרלוונטי בטור "דרישה".יש לנמק בטור "הסיבה לחוסר הרלוונטיות" את הסיבה לכך.

ב. שים לב! כל פרק 12 בשאלון הוא רלוונטי לכן **<u>אין</u>** לרשום V בטור "אחר" בפרק זה.ניתן רק לרשום V בתורים "כן" או "לא".

בהצלחה

הצהרת עמידה בתקן, שאלון A

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

חלק 2. תחום העיסוק של בית העסק (יש לסמן את כל הרלוונטיים):				
☐ קמעונאי	☐ טלקומוניקציה	☐ מרכולים/סופרמרקט		
☐ דלק	☐ מסחר אלקטרוני	☐ הזמנות דואר/טלפון	☐ אחר (אנא פרט):	
נא לציין מתקנים ואתרים הנכללים בסקר PCI DSS זה:				

חלק 2א. קשרים עסקיים		
האם לחברה קשרים עסקיים עם ספק שירותים צד ג' (REDIRECT) אחד או יותר (לדוגמה, שערי תקשורת, חברות אחסון אתרים, סוכני הזמנות של חברות תעופה, סוכנים של מועדוני לקוחות וכיו"ב)?	X כן	☐ לא
האם לחברה קשר עסקי עם יותר מחברת כרטיסי אשראי (חברת סליקה) אחת?	☐ כן	☐ לא

חלק 2ב: עמידה בקריטריונים למילוי שאלון A

בית העסק מאשר כי עומד בקריטריונים למילוי גרסה מקוצרת זו של שאלון הערכה עצמית מהנימוקים הבאים:

X	בית העסק אינו שומר, מעבד או משדר נתוני כרטיסי אשראי במערכות המחשוב שלו או במשרדיו אלא מסתמך לחלוטין על ספק(י) שירותים צד ג' לביצוע פעולות אלה;
X	ספק(י) השירותים צד ג' המטפל בשמירה, בעיבוד ו/או בשידור של נתוני כרטיסי האשראי הנו/ם גופ/ים המאושר/ים כעומד/ים בתקן PCI DSS;
X	בית העסק אינו שומר נתוני כרטיסי אשראי בפורמט אלקטרוני; **ובנוסף**
X	אם בית העסק בכל זאת שומר נתוני כרטיסי אשראי, מידע זה מופיע אך ורק על דוחות נייר וקבלות ואינו מתקבל בצורה אלקטרונית.

חלק 3. אשרור PCI DSS

בהסתמך על התוצאות שמצוינות בשאלון A מיום *(תאריך מילוי השאלון)*, *(שם בית העסק)* מאשר את סטטוס עמידה בתקן כדלקמן (יש לסמן אחד):

X	**עומד בתקן**: כל חלקי שאלון PCI SAQ מולאו וכל השאלות נענו בחיוב ולפיכך הדירוג הכללי של בית העסק הוא **עומד בתקן**, בהתאם לכך *(שם בית העסק)* הראה עמידה מלאה בדרישות תקן PCI DSS.
☐	**לא עומד בתקן:** לא מולאו כל חלקי שאלון PCI SAQ, או שישנן שאלות אשר נענו בשלילה, ולכן דירוגה הכללי של בית העסק הוא **לא עומד בתקן**, לפיכך *(שם בית העסק)* לא הראה עמידה מלאה בדרישות תקן PCI DSS.

חלק 3א. אישור סטאטוס עמידה בתקן	
בית העסק מאשר כי:	
שאלון הערכה עצמית A של PCI DSS, גרסה (מס' הגרסה של השאלון), הושלם בהתאם להוראות המופיעות בו.	X
כלל המידע הנכלל בתשובות לשאלון האמור לעיל ובהצהרה זאת מייצג בנאמנות את תוצאות הערכת העמידה בתקן שבצעתי.	X
קראתי את תקן PCI DSS ואני מכיר בזאת כי מחובתי להתמיד בעמידה בו.	X

חלק 3ב. אישור בית העסק

שם בית העסק:

_____

שם המנהל הבכיר בבית העסק:

_____

תפקיד:

_____

חתימה של מנהל בכיר בבית העסק:

_____

תאריך:

_____

הטמע אמצעי בקרת גישה חזקים

דרישה 9: הגבל גישה פיזית לנתוני כרטיסי האשראי

	שאלה	תשובה: כן	לא	אחר*
9.6	האם כל סוגי המדיה מאובטחים פיזית (לרבות, אך לא רק, מחשבים, מדיה אלקטרוניים ניידים, קבלות נייר, דוחות נייר ופקסים)? *למטרות דרישה 9, המונח "מדיה" מתייחס לכל הניירת והמדיה האלקטרונית המכילות נתוני כרטיסי אשראי.*	☐	☐	NA
9.7	(א) האם קיימת בקרה מחמירה על התפוצה הפנימית והחיצונית של כל סוגי המדיה?	☐	☐	NA
	(ב) האם הבקרות כוללות את הדברים הבאים :			
9.7.1	האם המדיה מסווגות כך שניתן לזהות מהי רמת הרגישות של המידע (המצוי בהן)?	☐	☐	NA
9.7.2	האם המדיה נשלחות באמצעות שליח מאובטח או בשיטת מסירה אחרת המאפשרת לעקוב אחריהן באופן מדויק?	☐	☐	NA
9.8	האם קיימים יומני רישום (לוגים) לצורך מעקב אחר כל המדיה המועברות מאזור מאובטח, והאם נדרש אישור מנהל לפני העברתן (במיוחד כשהן מופצות ליחידים)?	☐	☐	NA
9.9	האם יש שליטה קפדנית על אופן האחסון והנגישות למדיה ?	☐	☐	NA
9.10	האם כל המדיה מושמדות כאשר אין בהן עוד צורך עסקי או חוקי?	☐	☐	NA
	האם ההשמדה מתבצעת כדלהלן :			
9.10.1	(א) האם ניירת נגרסת בשיטת שתי וערב, נשרפת או נכתשת באופן שאינו מאפשר שחזור של נתוני כרטיסי האשראי?	☐	☐	NA
	(ב) האם מיכלים המאחסנים מידע המיועד להשמדה מאובטחים באופן המונע גישה לתכולתם? (למשל, התקנת מנעול על מיכל המכיל חומר לגריסה על מנת למנוע גישה לתכולתו).	☐	☐	NA

* אם סימנת V בטור "אחר" יש למלא נספח ד'.

החזק מדיניות אבטחת מידע

דרישה 12: החזק מדיניות אשר עונה על צרכי אבטחת המידע בקרב כל עובדך

	שאלה	תשובה: כן	לא	אחר*
12.8	אם נתוני כרטיסי אשראי מועברים לספקי שירות, האם קיימים ומוטמעים מדיניות ונהלים לניהול ספקי השירות, כדלהלן?			
12.8.1	האם ישנה רשימה מעודכנת של ספקי השירות?	X	☐	
12.8.2	האם קיים הסכם בכתב הכולל הכרה באחריותו של ספק השירות לאבטחת נתוני כרטיסי אשראי הנמצאים ברשותו?	X	☐	
12.8.3	האם קיים תהליך מסודר להתחלת העסקה של ספק שירות, לרבות בדיקת נאותות הולמת לפני העסקתו?	X	☐	
12.8.4	האם קיימת תכנית אשר עוקבת אחר סטאטוס העמידה בתקן PCI DSS של ספקי השרות?	X	☐	

* אם סימנת V בטור "אחר" יש למלא נספח ד'.

נספח ד': הסבר על חוסר רלוונטיות

במידה וסימנת V בתור "אחר", יש להשתמש בגיליון עבודה זה כדי לנמק מדוע הדרישה האמורה אינה רלוונטית לבית העסק.

דרישה	הסיבה לחוסר הרלוונטיות
דוגמה: *12.8*	*נתוני בעלי כרטיסי האשראי לעולם אינם מועברים לספקי שירות.*
חלק 9	לא רלוונטי כל המדיה מעובדת משודת ונשמרת ע"י ספק השירות אליו מבוצע REDIRECT