

חובת פיקוח על ספקים חיצוניים

תקן אבטחת נתונים בענף כרטיסי
התשלום (PCI DSS)

מדוע זה חשוב	תיאור	כותרת פיקוח
<p>הגנה על נתוני מחזיק הכרטיס: התקן המוכר להשגת המטרה הוא PCI DSS, והוא דרישה רגולטורית גלובלית בענף. תקני אבטחה מסוג PCI הם דרישות טכניות ותפעוליות שנקבעו על-ידי המועצה לתקני אבטחה של ענף כרטיסי התשלום כדי להגן על נתוני בעלי הכרטיס.</p>	<p>על הספק לציית לגרסאות הנוכחיות של תקני אבטחת הנתונים בענף כרטיסי התשלום כפי שהונפקו על-ידי מועצת תקני אבטחת התשלום, כגון PCI DSS, PA-DSS, PCI-P2PE, PCI-PTS, ייצור כרטיסי PCI.</p>	<p>השגת ציות לנתוני הכרטיס</p>
<p>הוכחה לכך שספק או סוחר מציינים באופן רלוונטי לנתוני כרטיס להיקף השירותים הניתנים ל- Barclays ועמדו בדרישות. הוכחה לכך שעדות הספק על RoC / AoC או SAQ קשורה לשירות המסופק.</p> <p>אם Barclays משתמשים בספקים או בסוחרים שאינם תואמים ל- PCI DSS, הם יידרשו ליצור קשר עם צוות הסיכון של צד שלישי של Visa Europe (agentcompliance@visa.com) באמצעות דוא"ל כדי לאשר שהספק או הסוחר מיישמים PCI DSS, וסיפקו ל- Visa Europe תוכנית סטטוס PCI DSS (באמצעות התבנית Visa Europe) לסקירה ולאישור של Visa Europe.</p>	<p>על הספק לספק אישור תאימות להערכות באתר (AoC), ובמידת הצורך, שאלון הערכה עצמית (SAQ), שרלוונטי להיקף השירותים הניתנים ל- Barclays, לפני חוזה ומדי שנה לאחר מכן. יש להתאים את האישור והשאלון לדרישות PCI DSS – למידע נוסף, באפשרותך לעיין באתר www.pcisecuritystandards.org</p> <p>אם סקירת ה- AoC מעלה שאלות כגון בנוגע להיקף השירותים, תיאור הסביבה או תאימות ה- PCI של הספק, ייתכן שהדוח הבסיסי על תאימות (RoC) יתבקש וייבדק לקבלת מידע נוסף. RoC ערוך עשוי להתקבל אם הוא מאשר את היקף אישור ה- PCI שחל על היקף השירותים הניתנים, או שאלות אחרות ש- Barclays העלתה לאחר סקירת ה- AoC.</p> <p>על הספק להודיע ל- Barclays כשהוא אינו מצייט עוד. כלומר, בהקדם האפשרי ולא יאוחר מ-30 ימים ממועד פקיעת מסמכי הציות.</p>	<p>אישור הספק והסוחר</p>

<p style="text-align: center;">מ-PCI DSS v3.2.1</p> <p>הליך בדיקה ל-12.8.2: יש להקפיד על הסכמים בכתב ולאשר שהם כוללים אישור של ספקי שירות שהם אחראים לאבטחת נתוני בעל הכרטיס שיש לספקי השירות או שהם מאחסנים, מעבדים או מעבירים בשם הלקוח בדרך אחרת, או במידה שהם עלולים להשפיע על האבטחה של סביבת הנתונים של בעל הכרטיס של הלקוח. הערה: בנוסף לדרישה 12.9, הדרישה להסכמים בכתב בין ארגונים וספקי שירות נועדה לקדם רמה עקבית של הבנה בין הצדדים על אחריות PCI DSS הרלוונטית. לדוגמה, ההסכם עשוי לכלול את דרישות PCI DSS הרלוונטיות שיש לשמור כחלק מהשירות המסופק.</p> <p>הנחיה ל-12.8.2: ההכרה של ספקי השירות מעידה על מחויבותם לשמירה על אבטחה מתאימה של נתוני בעל הכרטיס שהם מקבלים מלקוחותיהם. המדיניות וההליכים הפנימיים של ספק השירות שקשורים לתהליך מעורבות הלקוחות, ולכל התבניות שמשמשות להסכמים כתובים, צריכים לכלול מתן אישור PCI DSS רלוונטי ללקוחותיהם. יש להסכים על השיטה שבה ספק השירות מעביר אישור בכתב בין הספק ללקוחותיו.</p>	<p style="text-align: right;">אישור הספק</p> <p>על הספק לאשר בכתב ל-Barclays לפני חתימת החוזה שהוא אחראי על אבטחת נתוני בעל הכרטיס לשירותים הבאים שבבעלותו/שהוא מאחסן/מעבד/מעביר או יכולים להשפיע על האבטחה על סביבת הנתונים של מחזיק הכרטיס של לקוח Barclays כגון שירותי אבטחה (למשל שרתי אימות), אירוח מקוון וכו'.</p> <p>יש ליידע את Barclays בכתב על שינויים בשירות שסופק לפני ביצוע השינוי.</p>	
--	--	--

שימוש בספקי שירות של צד שלישי/מיקור חוץ

ספק שירות או סוחר עשויים להשתמש בספק שירות של צד שלישי כדי לאחסן, לעבד או לשדר נתונים מטעמם, או כדי לנהל רכיבים כגון נתבים, חומות אש, מסדי נתונים, אבטחה פיזית ו/או שרתים. לכן עשויה להיות השפעה על האבטחה של סביבת הנתונים של בעל הכרטיס.

על הצדדים לזהות בברור את השירותים ואת רכיבי המערכת הכלולים בהיקף הערכת PCI OSS של ספק השירות, דרישות PCI DSS ספציפיות שמכוסות על-ידי ספק השירות, ודרישות שהלקוחות של ספק השירות אחראים לכלול בסקירות PCI DSS משלהם, לדוגמה, על ספק אירוח מנוהל להגדיר בברור אילו מכתובות ה-IP שלו נסרקו כחלק מתהליך סריקת הפגיעות הרבעוני, ואילו כתובות IP הלקוח אחראי לכלול בסריקות הרבעוניות שלו.

ספקי השירות אחראים להציג את תאימות PCI DSS, וייתכן שיידרשו לעשות זאת באמצעות מותגי התשלום. על ספקי השירות ליצור קשר עם הרוכש ו/או מותג התשלום כדי לקבוע את אימות התאימות המתאים.

לרשות ספקי שירות של צד שלישי עומדות שתי אפשרויות לאימות תאימות:

- (1) **הערכה שנתית:** ספקי שירות יכולים לעבור הערכת PCI DSS שנתית בעצמם ולספק ראיות ללקוחותיהם כדי להוכיח את עמידתם; או
- (2) **הערכות מרובות לפי דרישה:** אם הם אינם עוברים הערכות PCI DSS שנתיות משלהם, על ספקי השירות לעבור הערכות בהתאם לבקשת הלקוחות, ו/או להשתתף בכל אחת מביקורות PCI DSS של לקוחותיהם, כשהתוצאות של כל בדיקה מסופקות ללקוח המתאים

אם הצד השלישי עובר הערכת PCI DSS משלו, עליו לספק ללקוחותיו מספיק ראיות כדי לוודא שהיקף הערכת PCI DSS של ספק השירות כיסה את השירותים שרלוונטיים ללקוח, ושדרישות PCI DSS הרלוונטיות נבדקו ונקבעו בהתאם. סוג הראיות הספציפיות שספק השירות מספק ללקוחותיו יהיה תלוי בהסכמים/חוזים הקיימים בין הצדדים. לדוגמה, אספקת ה-AOC ו/או הסעיפים הרלוונטיים של ה-ROC של ספק השירות (שנערכו כדי להגן על מידע סודי), יכולה לסייע לספק את כל המידע או חלק ממנו.

בנוסף, על סוחרים וספקי שירות לנהל ולנטר את הציות ל-PCI DSS של כל ספקי שירות מצד שלישי הקשורים עם גישה לנתוני בעלי הכרטיס. יש לעיין בדרישה 12.8 במסמך זה לקבלת פרטים.