

PCI staðalinn - hvaða sjálfsmat á við um minn rekstur?

Tegund

Sjálfsmat A

Útvistun kortaupplýsinga

Sjálfsmat B

Sjálfstæður Posi og þrykkivélur

Sjálfsmat C-VT

Vefposi (Virtual Terminal)

Sjálfsmat C

Greiðslulausnir/Posar sem tengjast Internetinu

Sjálfsmat D

Allir aðrir söluaðilar (en A-C) auk þjónustuaðila

Skilgreining

Öll meðhöndlun og vistun kortaupplýsinga í útvistun hjá þjónustuaðilum

Eingöngu sjálfstæða POSA eða notkun á þrykkivélum. Enginn geymsla á kortaupplýsingum á rafrænu formi.

Eingöngu "Vefposi" þar sem engin geymsla rafræna kortaupplýsinga á sér stað.

IP Posi eða greiðslulausn sem ekki geymir kortaupplýsingar á rafrænan hátt

Allir aðrir söluaðilar og þjónustuaðilar á kerfum söluaðila sem ber að svara sjálfsmati

Kröfur og nánari skilgreining á sjálfsmati

- Eingöngu viðskipti þar sem korthafi er ekki á staðnum
- Engin meðhöndlun á kortaupplýsingum í eigin kerfum, öll meðferð kortaupplýsinga í útvistun
- Þjónustuaðili er með PCI vottun
- Eingöngu geymdar kortakvittanir á pappír
- Engin geymsla á sér stað á kortaupplýsingum á rafrænu formi

- Eingöngu um að ræða sjálfstæða POSA (símatengdur) eða notkun á þrykkivélum
- Posinni er ekki á nokkurn hátt tengdur öðrum kerfum s.s. kassakerfi
- Posinn er ekki tengur við Internetið, heldur tengist við þjónustuaðila eða færsluhirði með venjulegri símalínu
- Engar kortaupplýsingar flæða yfir Internetið
- Einungis geymdar kortakvittanir á pappír
- Kortaupplýsingar ekki geymdar á rafrænu formi

- Vefposi sem er hýstur af þjónustuaðila eða færsluhirði, aðgangur er í gegnum Internet vafra Tölvukerfi söluaðila ekki tengt við önnur kerfi í hans umhverfi
- Sjálfstæður Vefposi án allra tenginga við aðra slíka posa
- PCI vottaður þjónustuaðili eða færsluhirðir útvegar og vistar vefposann.
- Engin hugbúnaður í kerfum söluaðila sem vistar eða meðhöndlar kortaupplýsingar
- Engin rafræn miðlun á kortaupplýsingum í kerfum söluaðila
- Einungis geymdar kortakvittanir á pappír
- Kortaupplýsingar ekki geymdar á rafrænu formi

- Posi eða greiðslulausn með internettengingu á sama tæki og/eða sama nærneti (LAN).
- Greiðslulausn eða internettenging tengist ekki öðrum kerfum innan netkerfis t.d. með því að einangra greiðslukerfi/ internet frá öðrum kerfum.
- Verslunareiningin er ekki tengd öðrum verslunareiningum og hvert nærnet (LAN) er einungis fyrir eina verslunareiningu
- Einungis geymdar kortakvittanir á pappír
- Kortaupplýsingar ekki geymdar á rafrænu formi
- Þjónustuaðili/færsluhirðir notar einungis öruggar fjartengingar við þjónustu á greiðslukerfinu

- Fyrirtæki sem svara/ uppfylla staðalinn samkvæmt D verða að uppfylla sérhvert atriði staðalsins.
- Í sumum tilvikum eiga spurningar ekki við umhverfi fyrirtækisins og því getur það ekki uppfyllt ákveðnar kröfur, dæmi: þegar fyrirtæki notar ekki þráðlaust net.
- Í þeim tilvikum þar sem spurningar eiga ekki við verður að verður að setja N/A (á ekki við) í dálkinn Special og útskýra sjóan ástæður þess í sérstöku eyðublaði í SAQ Appendix fyrir hvert atriði sem passa ekki við aðstæður fyrirtækisins.

Hlífing

Svara sjálfsmati A með 13 spurningum ásamt staðfestingu á sannleiksgildi svara (Attestation of Compliance).

Svara sjálfsmati B með 29 spurningum ásamt staðfestingu á sannleiksgildi svara (Attestation of Compliance).

Svara sjálfsmati C-VT með 51 spurningu ásamt staðfestingu á sannleiksgildi svara (Attestation of Compliance).

Svara sjálfsmati C með 40 spurningum ásamt staðfestingu á sannleiksgildi svara (Attestation of Compliance).

Svara sjálfsmati D með 288 spurningum ásamt staðfestingu á sannleiksgildi svara (Attestation of Compliance).

Skönnun

Öll fyrirtæki sem meðhöndla kortaupplýsingar á einhvern hátt ber að láta skanna allar almennar ip-tölur fyrirtækisins ársfjórðungslega.