

**Odvetvie platbných kariet   
Norma na ochranu údajov  
Samohodnotiaci dotazník B   
a preukazovanie zhody obchodníkov**

Obchodníci používajúci iba Imprinter alebo samostatný terminál, dial-up terminál – nearchivujú údaje držiteľa platobnej karty

**Na použitie s PCI DSS verzia 3.2**

Vydanie 1.1

**Zmeny v dokumente**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dátum** | **PCI DSS verzia** | **SAQ vydanie** | **Popis** |
| Október 2008 | 1.2 |  | Zosúladenie obsahu s novou verziu 1.2 PCI DSS a implementácia menších zmien zaznamenaných od pôvodnej verzie 1.1. |
| Október 2010 | 2.0 |  | Zosúladenie obsahu s novými požiadavkami na skúšobné postupy verzie 2.0 PCI DSS. |
| Február 2014 | 3.0 |  | Zosúladenie obsahu s novými požiadavkami na skúšobné postupy verzie 3.0 PCI DSS a zahrnutie dodatočných možností odozvy. |
| Apríl 2015 | 3.1 |  | Zosúladenie s PCI DSS v3.1. Podrobné informácie o zmenách PCI DSS sú uvedené v *PCI DSS - Súhrn zmien medzi verziami 3.0 a 3.1 PCI DSS.* |
| Júl 2015 | 3.1 | 1.1 | Odstránené odkazy na „osvedčené postupy" pred 30. júnom 2015 a odstránená možnosť podávania správ z v2 PCI DSS v bode 11.3 Požiadavky. |
| Apríl 2016 | 3.2 | 1.0 | Zosúladenie s PCI DSS v3.2. Podrobné informácie o zmenách PCI DSS sú uvedené v *PCI DSS - Súhrn zmien medzi verziami 3.1a 3.2PCI DSS.* |
| Január 2017 | 3.2 | 1.1 | Aktualizované číslovanie verzií na zosúladenie s inými SAQ |

**Obsah**

Zmeny dokumentu

Úvod

Samohodnotiaci postup PCI DCC

Vysvetlenie samohodnotiaceho dotazníku

Očakávané skúšky

Vyplnenie samohodnotiaceho dotazníku

Nepoužiteľnosť určitých špecifických požiadaviek

Vysvetlenie rozdielu medzi „nevzťahuje sa" a „netestované"

Právne výnimky

**Sekcia 1:** Informácie o hodnotení

**Sekcia 2:** Samohodnotiaci dotazník B pre obchodníkov

Vytváranie a udržiavanie bezpečnej siete a systémov

Ochrana údajov držiteľa karty

*Požiadavka 3:* Ochrana uložených údajov držiteľa karty

*Požiadavka 4:* Šifrovanie prenosových údajov držiteľa karty pri použití v otvorených verejných sietiach

Implementácia prísnych opatrení na kontrolu prístupu

*Požiadavka 7:* Obmedzenie prístupu k údajom držiteľa karty v nevyhnutnom rozsahu

*Požiadavka 9:* Obmedzenie fyzického prístupu k údajom držiteľa karty

Udržiavanie politiky zabezpečenia informácií

*Požiadavka 12:* Udržiavanie politiky, ktorá rieši bezpečnosť informácií všetkých pracovníkov

**Dodatok A:** Dodatočné požiadavky PCI DSS

*Dodatok A1:*  Dodatočné požiadavky PCI DSS pre spoločných poskytovateľov hostingu

*Dodatok A3:*  Dodatočná validácia určených subjektov (DESV)

**Dodatok B:** Hárok kompenzácií ovládacích prvkov

**Dodatok C:** Vysvetlenie pojmu „nevzťahuje sa"

**Odsek 3:** Podrobnosti o overovaní a osvedčovaní

**Úvod**

Systém SAQ B pre obchodníkov sa vzťahuje na obchodníkov, ktorí sú oprávnení využívať SAQ a ktorí nespĺňajú kritéria pre žiaden iný typ SAQ. Príklady takýto obchodníkov sú (vrátane, ale nielen):

 Elektronickí obchodníci, ktorí prijímajú údaje držiteľov karty na svojich webových stránkach.

 Obchodníci s elektronickým ukladaním údajov držiteľov karty

 Obchodníci, ktorí údaje držiteľa karty neukladajú elektronicky a zároveň nespĺňajú kritéria iného typu SAQ

 Obchodníci podnikajúci v prostredí, ktoré môže spĺňať kritéria iného typu SAQ ale ktoré má dodatočné požiadavky PCI DSS vzťahujúce sa na dané prostredie

Pričom množstvo organizácií vykonávajúcich SAQ B potrebuje overovať súlad s každou požiadavkou PCI DSS, niektoré organizácie s veľmi špecifickým obchodným modelom dokážu rozpoznať, že nie všetky požiadavky sa na ne vzťahujú. Pozrite pokyny nižšie pre podrobné informácie o vylúčení určitých špecifických požiadaviek.

**Samohodnotiaci postup PCI DCC**

1. Určite príslušné SAQ pre vaše prostredie - pre postup si pozrite dokument o pokynoch a usmerneniach k samohodnotiacemu dotazníku na webovej stránke PCI SSC.

2. Potvrďte, že vaše prostredie je správne zaradené a spĺňa kritéria oprávnenosti typu SAQ, ktorý používate.

3. Vyhodnoťte súlad vášho prostredia s požiadavkami PCI DSS.

4. Vyplňte všetky sekcie tohto dokumentu:

* Sekcia 1 (časti 1 a 2 AOC) - Informácie o hodnotení a zhrnutie.
* Sekcia 2 - Samohodnotiaci dotazník PCI DSS (SAQ B)
* Sekcia 3 (časti 3 a 4 AOC) - Údaje o overovaní a osvedčovaní a akčný plán pre nesplnené požiadavky (ak existujú)

5. Predložte vášmu nadobúdateľovi, kartovej spoločnosti alebo inému žiadateľovi SAQ osvedčenie o súlade (AOC) spolu s akoukoľvek ďalšou potrebnou dokumentáciou, ako sú naskenované správy ASV.

**Vysvetlenie samohodnotiaceho dotazníka**

Otázky obsiahnuté v stĺpci „otázka PCI DSS" v tomto samohodnotiacom dotazníku vychádzajú z požiadavky PCI DSS.

Odkazy na užitočné informácie o požiadavkách PCI DSS a spôsobe vyplnenia samohodnotiaceho dotazníka Vám boli zaslané spolu na uľahčenie hodnotiaceho procesu. Prehľad týchto odkazov je uvedený nižšie:

|  |  |
| --- | --- |
| **Dokument** | **Obsahuje:** |
| PCI DSS  *(Štandardné požiadavky na zabezpečenie údajov PCI a postupy hodnotenia bezpečnosti)* |  Pokyny na priraďovanie   Vysvetlenie zámeru všetkých požiadaviek PCI DSS   Podrobnosti o testovacích postupoch   Pokyny ku kompenzačným kontrolám |
| Dokumenty o pokynoch a usmerneniach SAQ |  Informácie o všetkých SAQ a kritériách oprávnenosti   Ako zistiť, ktorý SAQ sa vzťahuje na vašu organizáciu |
| *Slovník pojmov, skratky a akronymy PCI DSS a PA-DSS* |  Popis a definície pojmov použitých v PCI DSS a samohodnotiacich dotazníkoch |

Tieto a ďalšie zdroje je možné nájsť na webovej stránke PCI SSC *(www.pcisecuritystandards.org*). Odporúča sa, aby si organizácie preštudovali PCI DSS a iné podporné dokumenty pred začiatkom hodnotiaceho procesu.

***Očakávané testovanie***

Pokyny uvedené v stĺpci „očakávané testovanie" vychádzajú zo skúšobných postupov PCI DSS a poskytujú podrobný popis typov potrebných skúšobných činností na verifikáciu súladu s požiadavkami. Podrobné informácie o skúšobných postupoch pre každú požiadavku je možné nájsť v PCI DSS.

**Vyplnenie samohodnotiaceho dotazníka**

Pre každú otázku máte možnosť výberu odpovedí na označenie stavu vašej spoločnosti v súvislosti s touto požiadavkou. ***Vyberte len jednu odpoveď pre každú otázku.***

Popis významu každej odpovede je uvedený v nasledujúcej tabuľke:

|  |  |
| --- | --- |
| **Odpoveď** | **Kedy používať túto odpoveď:** |
| **Áno** | Očakávané testovanie bolo vykonané a všetky prvky požiadavky boli riadne splnené. |
| **Áno s CCW**  (Hárok kompenzačného riadenia) | Očakávané testovanie bolo vykonané a požiadavky boli splnené pomocou kompenzačného riadenia.  Všetky odpovede v tomto stĺpci vyžadujú vyplnenie hárku kompenzačného riadenia (CCW) obsiahnutého v prílohe B k SAQ.  Informácie o použití kompenzačných prvkov a pokyny o vyplnení hárku sú uvedené v PCI DSS. |
| **Nie** | Niektoré alebo všetky prvky požiadavky neboli splnené alebo sú v procese implementácie alebo vyžadujú dodatočné testovanie než je možné zistiť ich súlad. |
| **N/A**  (nevzťahuje sa) | Táto požiadavka sa nevzťahuje na prostredie organizácie. (Pozrite *Pokyny o neuplatňovaní špecifických požiadaviek* - príklady uvedené nižšie)  Všetky odpovede v tomto stĺpci vyžadujú dodatočné vysvetlenie podľa prílohy C k SAQ. |
| **Netestované** | Táto požiadavka nebola preskúmavaná v hodnotiacom procese a nebola žiadnym spôsobom testovaná. (Pozrite *Vysvetlenie rozdielu medzi pojmom „nevzťahuje sa" a „netestované"* - príklady, kedy je možné využiť túto možnosť). |

**Nepoužiteľnosť určitých špecifických požiadaviek**

Pričom množstvo organizácií vykonávajúcich SAQ B potrebuje overovať súlad s každou požiadavkou PCI DSS, niektoré organizácie s veľmi špecifickým obchodným modelom dokážu rozpoznať, že nie všetky požiadavky sa na ne vzťahujú. Napríklad od spoločnosti, ktorá nepoužíva bezdrôtovú technológiu v žiadnom rozsahu, sa neočakáva, že splní súlad so sekciami PCI DSS, ktoré sa špecificky venujú riadeniu bezdrôtovej technológie. Podobne organizácia, ktorá neukladá elektronicky žiadne údaje držiteľa karty, nemusí overovať požiadavky súvisiace s bezpečným ukladaním údajov držiteľa karty (napríklad požiadavky 3.4).

Príklady požiadaviek so špecifickou použiteľnosťou zahŕňajú:

 Otázky špecifické pre zabezpečenie bezdrôtových technológií (napríklad požiadavky 1.2.3, 2.1.1 a 4.1.1) musia byť zodpovedané len vtedy, ak je vo vašej sieti využívaná bezdrôtová technológia. Upozorňujeme, že požiadavka 11.1 (použitie procesov na identifikáciu neoprávnených bezdrôtových prístupových bodov) musí byť zodpovedaná, napriek tomu, že nevyužívate bezdrôtovú technológiu, keďže tento proces dokáže odhaliť akékoľvek neoprávnené alebo nepoctivé zariadenia nasadené bez vášho vedomia.

 Otázky týkajúce sa vývoja aplikácie a bezpečného kódovania (požiadavky 6.3 a 6.5) musia byť zodpovedané len, ak vaša organizácia vyvíja vlastné aplikácie.

 Otázky týkajúce sa požiadaviek 9.1.1 a 9.3 musia byť zodpovedané len pre zariadenia s „citlivými oblasťami" podľa tejto definície: „Citlivé oblasti" označujú akékoľvek dátové centrum, serverovú miestnosť alebo akúkoľvek oblasť, v ktorej sú umiestnené systémy na uchovávanie, spracovanie alebo prenášanie údajov držiteľa karty. Tým sa vylučujú oblasti, kde sú nainštalované predajné terminály, ako sú priestory pokladne v maloobchodnej predajni, avšak zahrnuté sú priestory serverových miestností, ktoré uchovávajú údaje držiteľa karty a iné priestory slúžiace na uchovávanie väčšieho množstva údajov držiteľov karty.

V prípade, že niektoré požiadavky sa považujú za neuplatniteľné vo vašom prostredí, vyberte možnosť „N/A" pre danú špecifickú požiadavku a vyplňte hárok „Vysvetlenie neuplatnenia" obsiahnutý v dodatku C pre každú odpoveď „N/A".

***Vysvetlenie rozdielu medzi „nevzťahuje sa" a „netestované"***

Neuplatnenie požiadavky na dané prostredie je nutné overiť samo o sebe. Použitím vyššie uvedeného príkladu, organizácia na to, aby vybrala „N/A" pre požiadavky 1.2.3, 2.1.1 a 4.1.1 musí najprv potvrdiť, že nepoužíva žiadnu bezdrôtovú komunikáciu vo svojej CDE a že žiadna taká sa nepripája na CDE. Po tomto potvrdení môže organizácia vybrať možnosť „N/A" pre tieto špecifické požiadavky.

V prípade, že požiadavka je úplne vylúčená z hodnotenia, bez akéhokoľvek skúmania o tom, či má byť uplatnená alebo nie, je nutné vybrať odpoveď „netestované". Príklady takýchto situácií môžu zahŕňať:

 Organizácia môže byť požiadaná svojim nadobúdateľom, aby overila skupinu požiadaviek, napríklad za pomoci prioritizovaného prístupu overovania určitých míľnikov.

 Organizácia chce potvrdiť novú bezpečnostnú kontrolu, ktorá ovplyvňuje iba určitú podmnožinu požiadaviek, napríklad implementáciu novej metodiky šifrovania, ktorá vyžaduje hodnotenie súladu s požiadavkami 2, 3 a 4 PCI DSS.

 Poskytovateľ služby môže ponúkať službu, ktorá pokrýva len určite množstvo požiadaviek PCI DSS, napríklad poskytovateľ fyzického skladovania môže vyžadovať validáciu fyzických bezpečnostných prvkov každej požiadavky 9 PCI DSS pre svoje skladovacie zariadenie.

V takýchto prípadoch môže organizácia overovať len určité požiadavky PCI DSS napriek tomu, že sa môžu na jej prostredie vzťahovať aj iné požiadavky.

**Právna výnimka**

V prípade, že vaša organizácia podlieha právnemu obmedzeniu, ktoré zabraňuje organizácii splniť požiadavky PCI DCC, zaškrtnite odpoveď „nie" pre danú požiadavku a vyplňte zodpovedajúce potvrdenie v časti 3.

**Sekcia 1:** **Informácie o hodnotení**

***Pokyny na predloženie***

Tento dokument musí byť vyplnený ako vyhlásenie o výsledkoch sebahodnotenia obchodníka so *Štandardnými* *bezpečnostnými požiadavkami platobných kariet a postupmi hodnotenia bezpečnosti (PCI DSS).* Vyplňte všetky sekcie: Obchodník je povinný zabezpečiť, aby každá sekcia bola vyplnená príslušnými stranami, podľa potreby. Obráťte sa na svojho nadobúdateľa (banku obchodníka) alebo kartové spoločnosti na určenie postupov podávania správ a predkladania.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Časť 1. Informácie o obchodníkovi a oprávnenom overovateľovi bezpečnosti** | | | | | | |
| **Časť 1a. Informácie o organizácii obchodníka** | | | | | | |
| Názov spoločnosti: | ........... | | DBA (obchodné meno): | ........... | | |
| Meno kontaktnej osoby: | ........... | | Titul: | ........... | | |
| Telefón: | ........... | | E-mail: | ........... | | |
| Obchodné sídlo: | ........... | | Mesto: | ........... | | |
| Štát / provincia: | ........... | Krajina: | ........... | | Poštové číslo: | ........... |
| URL: | ........... | | | | | |
| **Časť 1b. Informácie o oprávnenom overovateľovi bezpečnosti (podľa potreby)** | | | | | | |
| Názov spoločnosti: | ........... | | | | | |
| Meno kontaktnej osoby QSA: | ........... | | Titul: | ........... | | |
| Telefón: | ........... | | E-mail: | ........... | | |
| Obchodné sídlo: | ........... | | Mesto: | ........... | | |
| Štát / provincia: | ........... | Krajina: | ........... | | Poštové číslo: | ........... |
| URL: | ........... | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Časť 2. Súhrnná správa** | | | |
| **Časť 2a. Podnikateľská činnosť obchodníka (začiarknite všetky, ktoré sa vzťahujú)** | | | |
| Maloobchodník  Telekomunikácie  Potraviny a supermarkety | | | |
| Ropné výrobky  Elektronický predaj  Poštový / telefonický predaj (MOTO) | | | |
| Iné (uveďte): ........... | | | |
| Aké platobné metódy využíva vaša spoločnosť?  Poštové / telefonické objednávky (MOTO)  Elektronický predaj  Fyzická prítomnosť karty (kamenný predaj) | | Aké platobné metódy sú pokryté v tomto SAQ?  Poštové / telefonické objednávky (MOTO)  Elektronický predaj  Fyzická prítomnosť karty (kamenný predaj) | |
| ***Poznámka:*** *V prípade, že vaša spoločnosť využíva platobnú metódu alebo postup, ktoré nie sú obsiahnuté v tomto SAQ, obráťte sa na vášho nadobúdateľa alebo kartovú spoločnosť o validáciu ostatných metód.* | | | |
| **Časť 2b. Popis spracovania platobných kariet** | | | |
| Ako a v akom rozsahu vaša spoločnosť ukladá, spracováva a/alebo prenáša údaje držiteľa karty? | ........... | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Časť 2c. Miesta** | | | | |
| Uveďte zoznam všetkých zariadení (napríklad maloobchodné predajne, firemné kancelárie, dátové centrá, call centrá, atď.) a súhrn miest obsiahnutých v posudku PCI DSS. | | | |
| **Spôsob zariadenia** | **Počet zariadení tohto typu** | **Miesto zariadenia (mesto, krajina)** |
| *Príklad: Maloobchodné predajne* | *3* | *Boston, MA, USA* |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |
| ........... | ........... | ........... |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Časť 2d. Platobná aplikácia** | | | | | |
| Využíva vaša spoločnosť jednu alebo viacero platobných aplikácií? Áno Nie | | | | |
| Uveďte nasledujúce informácie týkajúce sa platobných aplikácií používaných vašou spoločnosťou: | | | | | |
| **Názov platobnej aplikcáie** | **Číslo verzie** | **Dodávateľ aplikácie** | **Je aplikácia v zozname PA-DSS?** | **Dátum skončenia platnosti PA-DSS (ak existuje)** | |
| ........... | ........... | ........... | Áno  Nie | ........... | |
| ........... | ........... | ........... | Áno  Nie | ........... | |
| ........... | ........... | ........... | Áno  Nie | ........... | |
| ........... | ........... | ........... | Áno  Nie | ........... | |
| ........... | ........... | ........... | Áno  Nie | ........... | |

|  |  |  |
| --- | --- | --- |
| **Časť 2e. Popis prostredia** | | |
| Uveďte ***podrobný*** popis prostredia posudzovaného v tomto hodnotení.  *Napríklad:*  • *Spojenia s dátovým prostredím držiteľa karty (CDE).*  • *Kritické súčasti systému v rámci CDE, ako sú POS, zariadenia, databázy, webové servery, atď. a akékoľvek ďalšie potrebné platobné komponenty, podľa potreby.* | ........... | | |
| Využíva vaša spoločnosť segmentáciu siete na zmenu rozsahu vášho prostredia PCI DSS?  *(Pozri sekciu „segmentácia siete" PCI DSS pre inštrukcie k segmentácii siete)* | | Áno  Nie | |

|  |  |  |
| --- | --- | --- |
| **Časť 2f. Poskytovateľ služieb v úlohe tretej strany** | | |
| Využíva vaša spoločnosť QIR (Kvalifikovaný integrátor a predajca)?  Ak áno:  Názov spoločnosti QIR: ...........  Samostatné meno QIR: ...........  Popis služieb poskytovaných QIR: ........... | | Áno  Nie | |
| Zdieľa vaša spoločnost údaje držiteľa karty s inými poskytovateľmi tretej strany (napríklad: QIR, poskytovatelia brán, spracovateľkých platobných služieb, platobných služieb (PSP) a webhostingových služieb, zástupcovia rezervačných leteckých služieb, zástupcovia vernostných programov, atď.)? | | Áno  Nie | |
| ***Ak áno:*** | | |
| **Meno poskytovateľa:** | **Popis poskytovnaých služieb:** | |
| ........... | ........... | |
| ........... | ........... | |
| ........... | ........... | |
| ........... | ........... | |
| ........... | ........... | |
| ........... | ........... | |
| ***Poznámka:*** *Požiadavky 12.8 sa vzťahujú na všetky subjekty v tomto zozname.* | | |

**Sekcia 2:** **Samohodnotiaci dotazník B pre obchodníkov**

***Poznámka:***Nasledujúce otázky sú očíslované podľa požiadavky PCI DSS a skúšobných postupov, ako sú definované v dokumente Požiadavky PCI DSS a postup hodnotenia bezpečnosti.

**Dátum dokončenia samohodnotenia:**

**Vybudovanie a udržiavanie bezpečnostnej siete a systémov**

***Požiadavka 1:*** ***Inštalácia a udržiavanie firewallového systému na ochranu dát***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |

**Ochrana údajov držiteľa karty**

***Požiadavka 3:*** ***Ochrana uložených údajov držiteľa karty***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 3.2 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | (c) Sú po dokončení autorizačného procesu citlivé autentifikačné údaje neobnoviteľné po ich vymazaní? |  Kontrola pravidiel a postupov   Preskúmanie systémových konfigurácií   Kontrola postupov mazania |  |  |  |  |  |
|  | (d) Spĺňajú všetky systémy nasledovné požiadavky týkajúce sa neuchovávania citlivých autentifikačných údajov po autorizačnom procese (aj keď sú zašifrované): |  |  |  |  |  |  |
| 3.2.1 | Neuchováva sa po autorizácii celý obsah akejkoľvek stopy (či už z magnetického prúžku umiestneného na zadnej strane karty, ekvivalentné údaje obsiahnuté na čipe alebo inak)?  *Tieto údaje sa alternatívne nazývajú celá stopa, stopa, stopa 1, stopa 2 a údaje z magnetického prúžku.*  ***Poznámka:*** *Pri bežnom podnikaní môže byť potrebné uchovať nasledujúce údaje z magnetického prúžku:*   *meno držiteľa karty,*   *číslo primárneho účtu (PAN),*   *dátum expirácie a*   *servisný kód*  *Na minimalizáciu rizika sú obvykle potrebné len tieto údaje.* |  Kontrola zdrojov údajov, vrátane:   údajov o prichádzajúcich transakciách   všetkých záznamoch   súborov histórie   súborov trasy   databázovej schémy   databázového obsahu |  |  |  |  |  |
| 3.2.2 | Overovací kód alebo hodnota na karte (trojmiestny alebo štvormiestny kód na prednej alebo zadnej strane platobnej karty) sa neukladá po autorizácii? |  Kontrola zdrojov údajov, vrátane:   údajov o prichádzajúcich transakciách   všetkých záznamoch   súborov histórie   súborov trasy   databázovej schémy   databázového obsahu |  |  |  |  |  |
| 3.2.3 | Osobné identifikačné číslo (PIN) alebo šifrovaný blok PIN sa neukladá po autorizácii? |  Kontrola zdrojov údajov, vrátane:   údajov o prichádzajúcich transakciách   všetkých záznamoch   súborov histórie   súborov trasy   databázovej schémy   databázového obsahu |  |  |  |  |  |
| 3.3 | Dochádza k maskovaniu kódu PAN pri jeho zobrazení (maximálne môže byť zobrazených prvých 6 čísiel a posledné 4 čísla) tak, aby boli zamestnanci schopní vidieť len prvých 6/posledné 4 čísla kódu PAN?  ***Poznámka:*** *Táto požiadavka nenahrádza prísnejšie požiadavky na zobrazovanie údajov držiteľov kariet - napríklad zákonné požiadavky alebo požiadavky kartovej spoločnosti na používanie kariet v mieste predaja (POS).* |  Kontrola pravidiel a postupov   Kontrola úloh, ktoré potrebujú prístup na zobrazenie plného kódu PAN   Preskúmanie systémových konfigurácií   Kontrola zobrazovania kódu PAN |  |  |  |  |  |

***Požiadavka 4:*** ***Šifrovanie prenosových údajov držiteľa karty pri použití v otvorených verejných sietiach***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 4.2 |  |  |  |  |  |  |  |
|  | (b) Sú zavedené pravidlá, ktoré stanovujú, aby nechránené kódy PAN nemohli byť posielané prostredníctvom systému odosielania správ koncového užívateľa? |  Kontrola pravidiel a postupov |  |  |  |  |  |

**Implementácia prísnych opatrení na kontrolu prístupu**

***Požiadavka 7:*** ***Obmedzenie prístupu k údajom držiteľa karty v nevyhnutnom rozsahu***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 7.1 | Je prístup k systémovým komponentom a údajom držiteľov kariet obmedzený len na tých oprávnených zamestnancov, a to nasledovne: |  |  |  |  |  |  |
| 7.1.2 | Je prístup k privilegovaným užívateľským ID obmedzeným nasledovne:   Najmenší potrebný rozsah na vykonávanie svojej pracovnej funkcie?   Priradený len na úlohy, ktoré špecificky vyžadujú privilegovaný prístup? |  Rozhovor s personálom   Rozhovor s manažmentom   Kontrola privilegovaných užívateľských ID |  |  |  |  |  |
| 7.1.3 | Priradenie prístupu na základe klasifikácie a funkcie jednotlivých zamestnancov? |  Rozhovor s manažmentom   Kontrola užívateľských ID |  |  |  |  |  |

***Požiadavka 9:*** ***Obmedzenie fyzického prístupu k údajom držiteľa karty***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 9.5 | Sú všetky médiá fyzicky zabezpečené (vrátane, ale nielen, počítačov, vymeniteľných elektronických médií, písomných dokladov, písomných správ a faxov)?  *Na účely požiadavky 9 „médiá" znamenajú písomné a elektronické média obsahujúce údaje držiteľov kariet.* |  Preskúmanie pravidiel a postupov fyzického zabezpečovania médií   Rozhovor s personálom |  |  |  |  |  |
| 9.6 | (a) Je udržiavaná prísna kontrola nad internou alebo externou distribúciou akéhokoľvek média? |  Preskúmanie pravidiel a postupov distribúcie médií |  |  |  |  |  |
| (b) Obsahujú kontroly nasledovné prvky: |  |  |  |  |  |  |
| 9.6.1 | Je médium klasifikované podľa citlivosti svojich údajov? |  Preskúmanie pravidiel a postupov klasifikácie médií   Rozhovor s bezpečnostným personálom |  |  |  |  |  |
| 9.6.2 | Sú média zasielané bezpečnou kuriérskou službou alebo iným spôsobom doručenia, ktorý je možné presne sledovať? |  Rozhovor s personálom   Kontrola sledovacích protokolov a dokumentácie distribúcie médií |  |  |  |  |  |
| 9.6.3 | Dochádza k schvaľovaniu prenosu médií zo strany manažmentu (predovšetkým, ak sú médiá distribuované jednotlivcom)? |  Rozhovor s personálom   Kontrola sledovacích protokolov a dokumentácie distribúcie médií |  |  |  |  |  |
| 9.7 | Je zachovaná prísna kontrola sledovania a dostupnosti médií? |  Kontrola pravidiel a postupov |  |  |  |  |  |
| 9.8 | (a) Dochádza k zničeniu médií, keď už nie sú potrebné z obchodných alebo právnych dôvodov? |  Kontrola pravidiel a postupov týkajúcich sa pravidelných likvidácií nepotrebných médií |  |  |  |  |  |
|  | (c) Likvidácia médií prebieha nasledovne: |  |  |  |  |  |  |
| 9.8.1 | (a) Sú písomné materiály rozrezané, spálené alebo rozdrvené tak, aby nebolo možné tieto písomné kópie žiadnym spôsobom rekonštruovať? |  Rozhovor s personálom   Preskúmanie procesov   Kontrola procesov |  |  |  |  |  |
| (b) Sú skladové kontajnery použité na skladovanie materiálov s informáciami zabezpečené voči neoprávnenému prístupu k obsahu? |  Kontrola bezpečnosti skladových kontajnerov |  |  |  |  |  |
| 9.9 | Sú zariadenia, ktoré zhromažďujú údaje držiteľov kariet prostredníctvom fyzickej interakcie s kartou chránené pred neoprávneným zásahom a nahradením, a to nasledovným spôsobom?  ***Poznámka:*** *Táto požiadavka sa týka zariadení na čítanie kariet, ktoré sa používajú pri transakciách s fyzickou kartou (vloženie alebo priloženie karty) v mieste predaja. Táto požiadavka sa neuplatňuje na ručné vstupné komponenty, ako sú počítačové klávesnice alebo klávesnice v mieste predaja.* |  |  |  |  |  |  |
| (a) Uvádzajú pravidlá a postupy nutnosť viesť zoznam takýchto zariadení? |  Kontrola pravidiel a postupov |  |  |  |  |  |
| (b) Uvádzajú pravidlá a postupy nutnosť vykonávania pravidelnej kontroly takýchto zariadení na odhalenie neoprávneného zásahu alebo výmeny? |  Kontrola pravidiel a postupov |  |  |  |  |  |
| (c) Uvádzajú pravidlá a postupy nutnosť zaškolenia personálu, aby vedel rozpoznávať podozrivé správanie a ohlasovať neoprávnené zásahy do zariadení? |  Kontrola pravidiel a postupov |  |  |  |  |  |
| 9.9.1 | (a) Obsahuje zoznam zariadení nasledovné položky?   Názov, model zariadenia   Umiestnenie zariadenia (napríklad adresa pracoviska alebo závodu, kde je zariadenie umiestnené)   Sériové číslo zariadenia alebo iný jedinečný identifikačný údaj |  Kontrola zoznamu zariadení |  |  |  |  |  |
| (b) Je zoznam presný a aktuálny? |  Kontrola zariadení a umiestnení zariadenia a porovnanie so zoznamom |  |  |  |  |  |
| (c) Je zoznam zariadení aktualizovaný po pridaní, premiestnení alebo vyradení zariadenia, atď.? |  Rozhovor s personálom |  |  |  |  |  |
| 9.9.2 | (a) Sú povrchy zariadení pravidelne kontrolované na odhalenie neoprávnených zásahov (napríklad pridaním skimmerov k zariadeniam) alebo výmene (napríklad kontrolou sériového čísla alebo inej identifikácie zariadenia, či nedošlo k jeho výmene), a to nasledovne?  ***Poznámka:*** *Príklady znakov, ktoré poukazujú na prípadné neoprávnené zásahy alebo výmeny, môžu zahŕňať podozrivé prípojné zariadenia alebo káble vsunuté do zariadenia, chýbajúce alebo zmenené bezpečnostné značky, poškodený alebo farebne odlišný kryt alebo nezrovnalosti v sériovom čísle zariadenia alebo iných vonkajších značiek.* |  Rozhovor s personálom   Preskúmanie kontrolných procesov a porovnanie so stanovenými postupmi |  |  |  |  |  |
| (b) Bol personál oboznámený s postupmi na kontrolu zariadení? |  Rozhovor s personálom |  |  |  |  |  |
| 9.9.3 | Bol personál vyškolený, aby vedel rozpoznať prípadné pokusy o neoprávnené zásahy alebo výmeny zariadení, a to nasledovne? |  |  |  |  |  |  |
| (a) Obsahujú školiace materiály pre pracovníkov v mieste predaja nasledovné informácie?   Verifikácia totožnosti tretích osôb, ktoré tvrdia, že vykonávajú servisné alebo údržbárske služby, predtým, než získajú prístup k zariadeniu.   Nemontujte, nevymieňajte a nevracajte zariadenia bez predošlého overenia.   Všímajte si podozrivé správanie okolo zariadení (napríklad pokusy o odpojenie alebo otvorenie zariadení neznámymi osobami).   Ohláste podozrivé chovanie a náznaky neoprávnených zásahov alebo výmien zariadení príslušným zamestnancom (napríklad manažérovi alebo bezpečnostnému pracovníkovi). |  Preskúmajte školiace materiály |  |  |  |  |  |
|  | (b) Prešiel personál predajného miesta školením o postupoch na odhaľovanie a hlásenie neoprávnených zásahov a výmien (alebo ich pokusov) zariadení? |  Rozhovor so zamestnancami na predajných miestach |  |  |  |  |  |

**Udržiavanie politiky**

**zabezpečenia informácií**

***Požiadavka 12:*** ***Udržiavanie politiky, ktorá rieši bezpečnosť informácií všetkých pracovníkov***

***Poznámka:*** *Na účely požiadavky 12 sa pod pojmom „personál" rozumejú zamestnanci na plný úväzok alebo čiastočný úväzok, zamestnanci na dohodu, dodávatelia a konzultanti, ktorí vykonávajú svoju činnosť v priestoroch subjektu alebo ktorí majú iný prístup k dátovému prostrediu držiteľov kariet.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Otázka PCI DSS** | | **Očakávané testovanie** | **Odpoveď**  ***(Zaškrtnite jednu odpoveď pre každú otázku)*** | | | | |
| **Áno** | **Áno s CCW** | **Nie** | **N/A** | **Netestované** |
| 12.1 | Je zavedená, zverejnená, udržiavaná a rozširovaná bezpečnostná politika pre celý personál? |  Kontrola informačnej bezpečnostnej politiky |  |  |  |  |  |
| 12.1.1 | Je bezpečnostná politika revidovaná raz ročne a aktualizovaná pri zmene prostredia? |  Kontrola informačnej bezpečnostnej politiky   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3 | Sú použité pravidlá pre kritické technológie vypracované tak, aby stanovovali použitie týchto technológií a vyžadovali:  ***Poznámka:*** *Príklady kritických technológií zahŕňajú, ale nie sú obmedzené na vzdialené prístupy a bezdrôtové technológie, notebooky, tablety, vymeniteľné elektronické médiá, či používanie emailov a internetu.* |  |  |  |  |  |  |
| 12.3.1 | Výslovný súhlas autorizovaným stranám na použitie technológií? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3.3 | Zoznam zariadení a personálu s prístupom? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.3.5 | Prijateľne používanie technológií? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
|  | (b) Pre personál s riadnym oprávneným, vyžadujú tieto pravidlá ochranu údajov držiteľov kariet v súlade s požiadavkami PCI DSS? |  Kontrola pravidiel používania   Rozhovor so zodpovedným personálom |  |  |  |  |  |
| 12.4 | Sú v bezpečnostnej politike a postupoch jasne stanovené zodpovednosti za bezpečnosť informácií pre všetkých pracovníkov? |  Kontrola informačnej bezpečnostnej politiky a postupov   Rozhovor s náhodnými zodpovednými zamestnancami |  |  |  |  |  |
| 12.5 | (a) Je formálne priradená zodpovednosť za informačnú bezpečnosť hlavnému bezpečnostnému riaditeľovi alebo inému manažérovi v oblasti bezpečnosti? |  Kontrola informačnej bezpečnostnej politiky a postupov |  |  |  |  |  |
| (b) Sú nasledujúce zodpovednosti informačného bezpečnostného manažmentu priradené jednotlivcovi alebo tímu: |  |  |  |  |  |  |
| 12.5.3 | Zriaďovanie, dokumentovanie a distribúcia odoziev na bezpečnostné incidenty a postupov eskalácie na zabezpečenie včasného a efektívneho zvládnutia všetkých situácií? |  Kontrola informačnej bezpečnostnej politiky a postupov |  |  |  |  |  |
| 12.6 | (a) Je zavedený formálny program na zvyšovanie povedomia o bezpečnosti tak, aby bol celý personál oboznámený o bezpečnostnej politike a postupoch v oblasti ochrany dát držiteľov kariet? |  Kontrola programu na zvyšovanie povedomia o bezpečnosti |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 12.8 | Sú udržiavané a implementované pravidlá a postupy tak, aby adresovali poskytovateľov služieb, s ktorými zdieľate údaje držiteľov kariet alebo ktorí by mohli narušiť bezpečnosť údajov držiteľov kariet, a to nasledovne: |  |  |  |  |  |  |
| 12.8.1 | Je udržiavaný zoznam poskytovateľov služieb, vrátane popisu poskytovaných služieb? |  Kontrola pravidiel a postupov   Kontrola procesov   Kontrola zoznamu poskytovateľov služieb |  |  |  |  |  |
| 12.8.2 | Sú udržiavané písomné dohody obsahujúce potvrdenie o tom, že poskytovatelia služieb nesú zodpovednosť za bezpečnosť údajov držiteľov kariet, ktoré sú im poskytnuté a ktoré uschovávajú, spracovávajú alebo zasielajú v mene zákazníka, alebo v rozsahu, v ktorom môžu narušiť bezpečnosť dátového prostredia držiteľov kariet?  ***Poznámka:*** *Presné znenie tohto potvrdenia záleží od dohody medzi oboma stranami, podrobností poskytovaných služieb a zodpovedností pridelených každej strane. Toto potvrdenie nemusí obsahovať presné znenie uvedené v tejto požiadavke.* |  Kontrola písomných dohôd   Kontrola pravidiel a postupov |  |  |  |  |  |
| 12.8.3 | Je zavedený postup na zabezpečenie dodržiavania bezpečnostných pravidiel zo strany poskytovateľov služieb, vrátane náležitej starostlivosti? |  Kontrola procesov   Preskúmanie pravidiel a postupov a podpornú dokumentáciu |  |  |  |  |  |
| 12.8.4 | Je udržiavaný program na monitorovanie súladu poskytovateľov služieb s požiadavkami PCI DSS najmenej raz ročne? |  Kontrola procesov   Preskúmanie pravidiel a postupov a podpornú dokumentáciu |  |  |  |  |  |
| 12.8.5 | Sú uchovávané informácie o tom, ktoré požiadavky PCI DSS sú riadené poskytovateľmi a ktoré sú riadené daným subjektom? |  Kontrola procesov   Preskúmanie pravidiel a postupov a podpornú dokumentáciu |  |  |  |  |  |
| 12.10.1 | (a) Bol vytvorený plán reakcie na incidenty v prípade narušenia systému? |  Kontrola plánu reakcie na incidenty   Kontroly postupov plánu reakcie na incidenty |  |  |  |  |  |

**Dodatok A:** **Dodatočné požiadavky PCI DSS**

***Dodatok A1:***  ***Dodatočné požiadavky PCI DSS pre spoločných poskytovateľov hostingu***

Tento dodatok sa nepoužíva na hodnotenie obchodníkov.

***Dodatok A3:***  ***Dodatočná validácia určených subjektov (DESV)***

Tento dodatok sa vzťahuje iba na subjekty vybrané kartovou spoločnosťou alebo nadobúdateľom, od ktorých sa vyžaduje dodatočné overenie požiadaviek PCI DSS. Subjekty, ktoré sú povinné overiť súlad podľa tohto dodatku by mali používať dodatočnú oznamovaciu šablónu DESV a dodatočné preukazovanie zhody a konzultovať proces predkladania s príslušnou kartovou spoločnosťou a/alebo nadobúdateľom.

**Dodatok B:** **Hárok kompenzačného riadenia**

*Použite tento hárok na stanovenie kompenzačného riadenia všetkých požiadaviek, kde ste vybrali „ÁNO s CCW".*

***Poznámka:*** *Len spoločnosti, ktoré vykonali analýzu rizík a ktoré majú oprávnené technologické alebo obchodné obmedzenia, môžu zvážiť použitie kompenzačného riadenia na dosiahnutie súladu.*

*Pozri dodatky B, C a D dokumentu PCI DSS pre informácie o kompenzačnom riadení a pokynoch na vyplnenie tohto hárku.*

**Číslo a popis požiadavky:** ...........

|  |  |  |
| --- | --- | --- |
|  | **Potrebné informácie** | **Vysvetlenie** |
| **1.** **Obmedzenia** | Zoznam obmedzení, ktoré zabraňujú dosiahnutie súladu s pôvodnou požiadavkou. | ........... |
| **2.** **Cieľ** | Stanoviť cieľ pôvodnej kontroly, identifikovať cieľ splnený kompenzačným riadením. | ........... |
| **3.** **Identifikácia rizika** | Identifikovať dodatočné riziká vyplývajúce z nedostatku pôvodnej kontroly. | ........... |
| **4.** **Stanovenie kompenzačného riadenia** | Stanovenie kompenzačného riadenia a vysvetlenie, akým spôsobom rieši cieľe pôvodnej kontroly a prípadné zvýšené riziká, ak existujú. | ........... |
| **5.** **Overenie kompenzačného riadenia** | Vysvetlenie spôsobu overenia a testovania kompenzačného riadenia. | ........... |
| **6.** **Údržba** | Stanovenie zavedených postupov a riadiacich prvkov na udržanie kompenzačného riadenia. | ........... |

**Dodatok C:** **Vysvetlenie pojmu „nevzťahuje sa"**

*V prípade zaškrtnutia stĺpca N/A („nevzťahuje sa") v dotazníku, použite hárok na vysvetlenie, prečo sa táto požiadavka nevzťahuje na vašu organizáciu.*

|  |  |
| --- | --- |
| **Požiadavka** | **Odôvodnenie, prečo sa požiadavka nevzťahuje** |
| *Príklad:* | |
| 3.4 | Údaje držiteľov kariet sa neukladajú elektronicky | |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |
| ........... | ........... |

**Odsek 3:** **Podrobnosti o overovaní a osvedčovaní**

|  |
| --- |
| **Časť 3. Overenie PCI DSS** |

**Tento AOC vychádza z výsledkov zaznamenaných v SAQ B (sekcia 2) zo dňa (*dátum dokončenia SAQ*).**

Na základe výsledkov zaznamenaných v SAQ B, signatári uvedení v častiach 3b-3d, podľa potreby, potvrdzujú nasledujúci súlad subjektu uvedeného v časti 2 tohto dokumentu: (***zaškrtnite jedno***):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Súlad:** Všetky sekcie PCI DSS SAQ sú dokončené, všetky otázky zodpovedané kladne, čo dáva výsledok **SÚLAD**, a preto (*meno spoločnosti obchodníka*) preukázal plný súlad s PCI DSS. | | | |
|  | **Nesúlad:** Nie všetky sekcie PCI DSS SAQ sú dokončené alebo nie všetky otázky zodpovedané kladne, čo dáva **NESÚLAD**, a preto (*meno spoločnosti obchodníka*) nepreukázal plný súlad s PCI DSS.  **Cieľový dátum** na dosiahnutie súladu: ...........  Od subjektu, ktorý predložil tento formulár so stavom Nesúlad, može byť požadované, aby dokončil akčný plán 4 v časti 4 tohto dokumentu. *Obráťte sa na svojho nadobúdateľa alebo kartovú spoločnosť pred vyplnením časti 4.* | | | |
|  | **Súlad s právnou výnimkou:** Jedna alebo viacero požiadaviek boli zaškrtnuté ako „Nie" v dôsledku zákonných obmedzení, ktoré zabránili splniť tieto požiadavky. Táto možnosť vyžaduje dodatočnú kontrolu zo strany nadobúdateľa alebo kartovej spoločnosti.  *Ak zaškrtnuté, vykonajte nasledovné:* | | | |
|  | **Dotknutá požiadavka** | **Podrobný opis zákonných obmedzení, ktoré zabraňujú dosiahnutie súladu s požiadavkou** |  |
| ........... | ........... |  |
| ........... | ........... |
|  | | |

|  |  |
| --- | --- |
| **Časť 3a. Potvrdenie stavu** | |
| **Podpis zodpovedných osôb:**  ***(hodiace sa zaškrtnite)*** | |
|  | Samohodnotiaci dotazník D PCI DSS, verzia (verzia SAQ) bol dokončený v zmysle uvedených pokynov. |
|  | Všetky informácie v rámci vyššie uvedeného SAQ a táto atestácia spravodlivo predstavujú výsledky hodnotenia vo všetkých významných aspektoch. |
|  | So svojim dodávateľom platobnej aplikácie som potvrdil, že môj platobný systém neukladá citlivé autentifikačné údaje po autentifikácií. |
|  | Prečítal som si PCI DSS a beriem na vedomie, že musím neustále dodržiavať požiadavky PCI DSS, ktoré sa vzťahujú na moje prostredie. |
|  | V prípade zmeny môjho prostredia beriem na vedomie, že musím prehodnotiť moje prostredie a implementovať dodatočné požiadavky PCI DSS, ktoré sa na neho môžu vzťahovať. |
| **Časť 3a. Potvrdenie stavu** (pokračovanie) | |
|  | V priebehu tohto hodnotenia nebol nájdený žiaden dôkaz o uchovávaných celých trasovacích údajoch alebo údajoch CAV2, CVC2, CID alebo CVV2 alebo PIN po autentifikácií transakcie na ŽIADNOM systéme posudzovanom v rámci tohto hodnotenia. |
|  | Kontroly ASV boli dokončené so schváleným skenovaním dodávateľa PCI SSC (*názov ASV*) |

|  |  |
| --- | --- |
| **Časť 3b. Atestácia obchodníka** | |
|  | |
| *Podpis výkonného riaditeľa obchodníka*  | *Dátum:* ........... |
| *Meno výkonného riaditeľa obchodníka:* ........... | *Titul:* ........... |

|  |  |  |
| --- | --- | --- |
| **Časť 3c. Informácie o oprávnenom overovateľovi bezpečnosti (QSA) (podľa potreby)** | | |
| V prípade, že do tohto hodnotiaceho procesu bol zapojený QSA, uveďte jeho úlohu: |  | |
|  | | |
| *Podpis riadne splnomocneného zástupcu spoločnosti QSA*  | | *Dátum:* ........... |
| *Meno riadne splnomocneného zástupcu:* ........... | | *Spoločnosť QSA:* ........... |

|  |  |
| --- | --- |
| **Časť 3d. Zapojenie interného overovateľa bezpečnosti (ISA) (podľa potreby)** | |
| V prípade, že do tohto hodnotiaceho procesu bol zapojený ISA, uveďte meno tohto zamestnanca a jeho úlohu: | ...........  ...........  ...........  ........... |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Časť 4. Akčný plán pre nevyhovujúce požiadavky** | | | | |
| Vyberte vhodnú akciu pre „Súlad s požiadavkami PCI DSS" pre každú požiadavku V prípade, že na niektorú z požiadaviek odpoviete „Nie", môže byť od vás požadované uviesť dátum, kedy vaša spoločnosť očakáva dosiahnutie súladu s touto požiadavkou a krátky popis krokov, ktoré podniknete na jej splnenie.  *Obráťte sa na svojho nadobúdateľa alebo kartovú spoločnosť pred vyplnením časti 4.* | | | | |
| **Požiadavka PCI DSS** | **Popis požiadavky** | **Súlad s požiadavkami PCI DSS**  (Vyberte jedno) | | **Dátum a iné opravné kroky** (Ak ste vybrali „nie" k akejkoľvek požiadavke) |
| **ÁNO** | **NIE** |
| 3 | Ochrana uložených údajov držiteľa karty |  |  | ........... |
| 4 | Šifrovanie prenosových údajov držiteľa karty pri použití v otvorených verejných sietiach |  |  | ........... |
| 7 | Obmedzenie prístupu k údajom držiteľa karty v nevyhnutnom rozsahu |  |  | ........... |
| 9 | Obmedzenie fyzického prístupu k údajom držiteľa karty |  |  | ........... |
| 12 | Udržiavanie politiky, ktorá rieši bezpečnosť informácií všetkých pracovníkov |  |  | ........... |

