AMERICAN EXPRESS

Provozní pravidla zabezpečení dat (DSOP)

Pruhy změn

Důležité aktualizace jsou uvedeny v Tabulce souhrnu změn a jsou také vyznačeny v DSOP pruhem změny. Pruhy změn jsou svislé čáry na levém okraji, které označují revidovaný, přidaný nebo odstraněný text. Všechny změny v DSOP jsou označeny pruhem změny, jak je ukázáno zde.

Tabulka souhrnu změn

Důležité aktualizace jsou uvedeny v následující tabulce a jsou také vyznačeny v *DSOP* pruhem změny.

Článek / pododdíl	Popis změny
Tato verze neobsahuje žádné změny.	

Jak si počínat, když máte Data incident?

Pokud jste ve své firmě zjistili Data incident, postupujte podle následujících kroků.

Krok č. 1:

Vyplňte Nahlašovací formulář Data incidentu obchodníka a pošlete ho e-mailem na adresu EIRP@aexp.com do 72 hodin od chvíle, kdy zjistíte, že k Data incidentu došlo.

Krok č. 2:

Důkladně záležitost vyšetřete; možná to bude vyžadovat objednání služeb Forenzního vyšetřovatele platebních karet (PCI).

Krok č. 3:

Neprodleně nám poskytněte všechna čísla kompromitovaných Karet American Express®.

Krok č. 4:

Spolupracujte s námi při řešení jakýchkoli problémů vyplývajících z Data incidentu.

Více podrobností o Povinnostech spojených s Data incidenty naleznete v Článku 3, „Povinnosti spojené s Data incidenty“.

Máte další otázky?

USA: (888) 732-3750 (bezplatný hovor)

Mezinárodní: +1 (602) 537-3021

EIRP@aexp.com

Jako špička v oblasti ochrany spotřebitelů se společnost American Express dlouhodobě zavazuje k ochraně Údajů držitelů karet a Citlivých ověřovacích údajů a zajištění jejich řádného zabezpečení.

Zneužití dat má negativní dopad na zákazníky, Obchodníky, Poskytovatele služeb a vydavatele karet. I jediná událost může výrazně poškodit pověst společnosti a negativně ovlivnit její schopnost efektivně podnikat. Minimalizace tohoto rizika prostřednictvím implementace provozních pravidel zabezpečení může zlepšit důvěru zákazníků, zvýšit výnosnost a vylepšit pověst společnosti.

Společnost American Express si je vědoma, že jako Obchodníci a Poskytovatelé služeb (společně **vy**) sdílíte naše obavy, a požaduje, abyste jako součást vašich povinností dodržovali ustanovení pro zabezpečení dat ve vaší **smlouvě** pro přijímání (v případě Obchodníků) nebo zpracování (v případě Poskytovatelů služeb) Karet American Express® (pro každého v příslušné Smlouvě) a ustanovení těchto Provozních pravidel zabezpečení dat, která můžeme čas od času pozměnit. Tyto požadavky platí pro veškeré vaše zařízení, systémy a sítě (a jejich součásti), na kterých jsou ukládány, zpracovávány či převáděny šifrovací klíče, Údaje držitelů karet či Citlivé ověřovací údaje (nebo jejich kombinace).

Termíny začínající velkým písmenem, které zde nejsou definovány, mají význam uvedený v glosáři na konci těchto pravidel.

Článek 1 Program cílené analýzy (TAP)

Zneužití údajů Držitelů karet může být způsobeno mezerami v zabezpečení dat ve vašem Prostředí údajů Držitelů karet (CDE).

Mezi příklady zneužití Údajů držitelů karet patří například:

- **Společné nákupní místo (CPP):** Držitelé karty American Express hlásí podvodné Transakce na účtech jejich Karet; tyto transakce jsou identifikovány a určeny jako transakce, které mají původ v nákupech ve vašich Provozovnách.
- **Nalezené údaje platebních karet:** Údaje Karet American Express a Údaje držitelů karet nalezené v celosvětové internetové síti jsou spojeny s Transakcemi ve vašich Provozovnách.
- **Podezření na přítomnost malwaru:** Společnosti American Express má podezření, že používáte software infikovaný škodlivým kódem nebo zranitelný vůči takovému kódu.

Program cílené analýzy (TAP) má za účel identifikovat potenciální zneužití údajů Držitelů karet.

Poté, co od společnosti American Express obdržíte oznámení o možném zneužití údajů Držitelů karet, musíte splnit následující požadavky a zajistit, aby tak učinily i vaše Kryté strany.

- Musíte neprodleně zkontrolovat, zda se ve vašem prostředí CDE nevyskytují mezery v zabezpečení dat a pokud ano, musíte je odstranit.
  - Pokud zadáváte prošetřování prostředí CDE externím dodavatelům, musíte zajistit, aby je vaši externí dodavatelé provedli zevrubně.
- Po obdržení oznámení od společnosti American Express musíte předložit souhrnný přehled podniknutých nebo plánovaných opatření po kontrole, posouzení a/nebo nápravném úsilí.
- Musíte předložit aktualizované ověřovací dokumenty v souladu s PCI DSS, jak je uvedeno dále v části Článek 5, „Důležité pravidelné ověření vašich systémů“.
- Podle okolností musíte k inspekci vašeho prostředí CDE zapojit kvalifikovaného Forenzního vyšetřovatele PCI (PFI), pokud vy nebo vaše Krytá strana:
  - nemůžete vyřešit problém zneužití údajů Držitelů karet v přiměřeném časovém termínu, a to na základě rozhodnutí společnosti American Express, nebo
  - potvrdíte, že došlo k Data incidentu, a dodržíte požadavky uvedené v části Článek 3, „Povinnosti spojené s Data incidenty“.

Tabulka A-1: Poplatek za nedodržení pravidel TAP

Popis	Obchodník na Úrovni 1 nebo Poskytovatel služeb na Úrovni 1	Obchodník na Úrovni 2 nebo Poskytovatel služeb na Úrovni 2	Obchodník na Úrovni 3 nebo na Úrovni 4
Může být vyměřen poplatek za nedodržení pravidel, pokud závazky plynoucí z programu TAP nebudou splněny v prvním termínu.	25 000 USD	5 000 USD	1 000 USD
Může být vyměřen poplatek za nedodržení pravidel, pokud závazky plynoucí z programu TAP nebudou splněny v druhém termínu.	35 000 USD	10 000 USD	2 500 USD
Může být vyměřen poplatek za nedodržení pravidel, pokud závazky plynoucí z programu TAP nebudou splněny v třetím termínu. **POZNÁMKA:** *Poplatky za nedodržení pravidel mohou být aplikovány, dokud nebudou závazky splněny nebo dokud nebude vyřešen problém identifikovaný podle programu TAP.*	45 000 USD	15 000 USD	5 000 USD

Pokud nedodržíte své závazky plynoucí z programu TAP, bude mít společnost American Express právo požadovat kumulativní poplatky za nedodržení pravidel, zadržet platby a/nebo ukončit tuto Smlouvu.

Článek 2 Normy pro ochranu Šifrovacích klíčů, Údajů držitelů karet a Citlivých ověřovacích údajů

Musíte dodržovat a musíte zajistit, aby Kryté strany dodržovaly, následující požadavky:

- ukládat Údaje držitelů karet pouze k umožnění Transakcí prostřednictvím Karet American Express v souladu s ustanoveními a požadavky této Smlouvy;
- nejpozději do data účinnosti pro implementaci příslušné verze splňovat požadavky aktuální verze PCI DSS a dalších požadavků PCI SSC, platných pro vaše zpracování, ukládání nebo přenos Údajů držitelů karet a Citlivých ověřovacích údajů;
- při nasazování nového Zařízení pro zadání kódů PIN nebo Platebních aplikací (nebo obou) nebo jejich nahrazování používat pouze zařízení či aplikace Schválené PCI.

Veškeré záznamy o Platbách prostřednictvím karet American Express a o Kreditu držené podle této Smlouvy musíte chránit v souladu s těmito ustanoveními o zabezpečení údajů; tyto záznamy můžete používat pouze pro účely plnění vašich povinností vyplývajících z této Smlouvy a musíte je odpovídajícím způsobem chránit. Vůči společnosti American Express nesete finanční i jinou zodpovědnost za zajištění toho, že Kryté strany budou dodržovat tato ustanovení ohledně zabezpečení údajů (kromě prokazování dodržování těchto pravidel Krytými stranami v souladu s Článkem 5, „Důležité pravidelné ověření vašich systémů“, pokud není v tomto článku stanoveno jinak).

Článek 3 Povinnosti spojené s Data incidenty

Jakýkoliv Data incident musíte okamžitě oznámit společnosti American Express, v každém případě nejpozději do sedmdesáti dvou (72) hodin od jeho zjištění.

Za tímto účelem prosím kontaktujte Program hlášení incidentů společnosti American Express (*EIRP*) na telefonním čísle +1 (602) 537-3021 (+ značí mezinárodní předčíslí IDD pro mezinárodní přímou volbu čísla, pro hovor platí sazba pro mezinárodní hovory) nebo zašlete e-mail na adresu EIRP@aexp.com. Pro každý Data incident musíte určit svou kontaktní osobu. Kromě toho:

- Musíte provést důkladné forenzní vyšetřování všech takových Data incidentů.
- V případě Data incidentů týkajících se 10 000 nebo více unikátních Čísel karet musíte do vyšetřování zapojit Forenzního vyšetřovatele PCI (PFI), aby toto vyšetřování provedl do pěti (5) dnů od zjištění Data incidentu.
- Neupravená zpráva o forenzním vyšetřování musí být poskytnuta společnosti American Express do deseti (10) pracovních dnů od jejího dokončení.
- Musíte společnosti American Express urychleně poskytnout všechna Čísla zneužitých karet. Společnost American Express si vyhrazuje právo provést vlastní interní analýzu k identifikaci Čísel karet, kterých se týká Data Incident.

Zprávy o forenzním vyšetřování musí být vyplněny do aktuální Šablony závěrečné forenzní zprávy o incidentu dostupné u PCI. Tato zpráva musí zahrnovat forenzní hodnocení, zprávy o dodržování pravidel a veškeré další informace týkající se Data incidentu. Dále musí identifikovat příčinu Data incidentu, potvrdit, zda jste v době Data incidentu dodržovali PCI DSS, a ověřit vaši schopnost předejít dalším Data incidentům prostřednictvím (i) poskytnutí plánu pro nápravu všech nedostatků v dodržování PCI DSS a (ii) účasti v programu dodržování pravidel společnosti American Express (jak je popsáno níže). Na žádost společnosti American Express musíte poskytnout potvrzení Kvalifikovaného experta na zabezpečení (QSA) o tom, že nedostatky byly napraveny.

Bez ohledu na výše uvedené odstavce tohoto Článku 3, „Povinnosti spojené s Data incidenty“ platí následující:

- Společnost American Express může podle vlastního uvážení požadovat, abyste v případě Data incidentů týkajících se méně než 10 000 unikátních Čísel karet zapojili do vyšetřování Data incidentu Forenzního vyšetřovatele PFI. Veškeré takové vyšetřování musí být v souladu s požadavky uvedenými výše v tomto Článku 3, „Povinnosti spojené s Data incidenty“ a musí být dokončeno v časové lhůtě požadované společností American Express.
- Společnost American Express může podle vlastního uvážení samostatně zapojit Forenzního vyšetřovatele PFI, aby provedl vyšetřování jakéhokoli Data incidentu, a může vám účtovat náklady na toto vyšetřování.

Při nápravě jakýchkoli problémů vzniklých z Data incidentu se zavazujete spolupracovat se společností American Express. Musíte také se společností American Express konzultovat vaši komunikaci s Držiteli karty, kteří byli Data incidentem postiženi, a poskytovat společnosti American Express (případně také získat veškeré nutné souhlasy pro poskytnutí) všechny relevantní informace za účelem ověření vaší schopnosti předejít budoucím Data incidentům způsobem, který je v souladu s touto Smlouvou.

Bez ohledu na jakékoli jinak určené povinnosti ochrany důvěrných informací stanovené v této Smlouvě má společnost American Express právo sdělit informace o jakémkoli Data incidentu Držitelům karet, Vydavatelům, ostatním účastníkům v Síti American Express a veřejnosti v rozsahu vyžadovaném Příslušnými právními předpisy, soudními, administrativními či regulatorními nařízeními, vyhláškami, předvoláními, žádostmi, nebo jinými procesy s cílem zmírnit riziko podvodu nebo jiného poškození, nebo jinak v rozsahu odpovídajícímu provozování Sítě American Express.

Článek 4 Odškodnění v případě Data incidentu

Vaše povinnosti poskytnout společnosti American Express odškodnění v případě Data incidentu podle této Smlouvy budou určeny v souladu tímto Článkem 4, „Odškodnění v případě Data incidentu“, aniž by se společnost American Express vzdala jakýchkoli dalších práv a opatření. Navíc k případným povinnostem poskytnout odškodnění může být požadováno, abyste uhradili poplatek za nedodržení pravidel v oblasti Data incidentů, jak je popsáno níže v tomto Článku 4, „Odškodnění v případě Data incidentu“.

V případě Data incidentu, který se týká:

- 10 000 nebo více Čísel karet American Express a zároveň buď:
  - Citlivých ověřovacích údajů nebo
  - Data platnosti,

  musíte společnost American Express odškodnit s použitím sazby ve výši 5 USD za číslo účtu.

Společnost American Express však od vás nebude požadovat odškodnění v případě Data incidentů, které se týkají:

- méně než 10 000 Čísel karet American Express nebo
- více než 10 000 Čísel karet American Express při splnění těchto podmínek:
  - oznámili jste společnosti American Express tento Data incident podle Článku 3, „Povinnosti spojené s Data incidenty“,
  - v době Data incidentu jste dodržovali PCI DSS (což je potvrzeno vyšetřováním Data incidentu Forenzním vyšetřovatelem PFI), a
  - daný Data incident nebyl způsobem vaším protiprávním jednáním či protiprávním jednáním vašich Krytých stran.

Bez ohledu na výše uvedené odstavce tohoto Článku 4, „Odškodnění v případě Data incidentu“ platí následující: za jakýkoli Data incident, bez ohledu na počet postižených Čísel karet American Express, zaplatíte společnosti American Express poplatek za nedodržení pravidel v oblasti Data incidentů nepřesahující 100 000 USD za každý Data incident (což bude stanoveno společností American Express podle jejího vlastního uvážení) v případě, že nesplníte kteroukoli ze svých povinností stanovených v Článku 3, „Povinnosti spojené s Data incidenty“. Aby se předešlo pochybnostem, upozorňujeme, že celkový poplatek za nedodržení pravidel v oblasti Data incidentů, stanovený pro jakýkoli jednotlivý Data incident, nepřesáhne 100 000 USD.

Společnost American Express vyloučí ze svých výpočtů jakékoli Číslo karty American Express, kterého se týkal některý předchozí požadavek na odškodnění za Data incident vznesený v období dvanácti (12) měsíců před Dnem upozornění. Veškeré výpočty společnosti American Express podle této metodiky jsou konečné.

V souladu se Smlouvou vám může společnost American Express účtovat celou částku povinného odškodnění za Data incidenty nebo může odečíst částku z plateb, které vám společnost American Express poskytuje (nebo částku naúčtovat na váš bankovní účet).

Vaše povinnosti týkající se odškodnění za Data incidenty zde uvedené nebudou považovány za náhodné, nepřímé, spekulativní, následné, zvláštní, represivní nebo exemplární škody podle této Smlouvy za předpokladu, že tyto povinnosti nezahrnují škody týkající se nebo mající povahu ztráty zisku nebo výnosů, ztráty dobrého jména nebo ztráty obchodních příležitostí.

Podle vlastního uvážení může společnost American Express snížit povinnost odškodnění pro Obchodníky pouze za takové Data incidenty, které splňují každé z následujících kritérií:

- příslušné Technologie snižovaní rizik byly použity před Data incidentem a byly používány během celého Období data incidentu,
- bylo dokončeno důkladné vyšetřování v souladu s programem PFI (pokud nebylo písemně dohodnuto jinak),
- forenzní zpráva jasně uvádí, že Technologie snižování rizik byly použity ke zpracování, ukládání a/nebo přenosu dat v době Data incidentu, a
- neukládáte (a během celého Období Data incidentu jste neukládali) Citlivé ověřovací údaje ani jakékoli Údaje držitelů karet, které nebyly přeměněny v nečitelné údaje.

Pokud je k dispozici snížení výše odškodnění, stanoví se snížení vaší povinnosti odškodnění (kromě veškerých splatných poplatků za nedodržení pravidel) takto:

Tabulka A-2: Požadovaná kritéria pro snížení povinnosti odškodnění

Snížení povinnosti odškodnění	Požadovaná kritéria
Standardní snížení: 50 %	>75 % z celkového počtu Transakcí zpracováno na Čipových zařízeních[1] NEBO
	Technologie snižování rizik používána ve >75 % lokalit Obchodníka[2]
Rozšířené snížení: 75 % až 100 %	>75 % z celkového počtu Transakcí zpracováno na Čipových zařízeních[1] A TAKÉ >75 % lokalit Obchodníka používá jinou Technologii snižování rizik[2]

[1] Určeno podle interní analýzy společnosti American Express.

[2] Určeno podle vyšetřování Forenzním vyšetřovatelem PFI.

- Rozšířené snížení (75 % až 100 %) se určí na základě menšího procenta Transakcí s použitím Čipových zařízení A TAKÉ lokalit Obchodníka používajících jiné Technologie snižování rizik. Níže uvedené příklady ilustrují výpočet snížení odškodnění.
- Chcete-li splnit kritéria pro používání Technologie snižování rizik, musíte prokázat efektivní využití technologie v souladu s její klasifikací a zamýšleným účelem. Například nasazení Čipových zařízení a zpracování Čipových karet jako Transakcí s magnetickým proužkem nebo Transakcí se zadaným klíčem NENÍ efektivním využitím této technologie.
- Procento vašich lokalit, které používají Technologii snižování rizik, je určeno vyšetřováním Forenzním vyšetřovatelem PFI.
- Snížení povinnosti odškodnění se nevztahuje na žádné poplatky za nedodržení pravidel splatné v souvislosti s Data incidentem.

Tabulka A-3: Rozšířené snížení povinnosti odškodnění

Př.	Použití Technologií snižování rizik	Povinnosti odškodnění	Snížení
1	80 % Transakcí zpracováno na Čipových zařízeních	Ne	50 %: Standardní snížení (méně než 75% použití Technologií snižování rizik nestačí na splnění kritérií pro Rozšířené snížení)[1]
	0 % lokalit používá jinou Technologii snižování rizik		
2	80 % Transakcí zpracováno na Čipových zařízeních	Ano	77 %: Rozšířené snížení (na základě 77% použití Technologie snižování rizik)
	77 % lokalit používá jinou Technologii snižování rizik		
3	93 % Transakcí zpracováno na Čipových zařízeních	Ano	93 %: Rozšířené snížení (na základě zpracování 93 % Transakcí na Čipových zařízeních)
	100 % lokalit používá jinou Technologii snižování rizik		

Př.	Použití Technologií snižování rizik	Povinnosti odškodnění	Snížení
4	40 % Transakcí zpracováno na Čipových zařízeních	Ne	50 %: Standardní snížení (méně než 75 % Transakcí na Čipových zařízeních nestačí na splnění kritérií pro Rozšířené snížení)
	90 % lokalit používá jinou Technologii snižování rizik		

[1] Data incident týkající se 10 000 účtů Karet American Express, se sazbou 5 USD na každé číslo účtu (10 000 x 5 USD = 50 000 USD), může být způsobilý ke snížení ve výši 50 %, čímž se sníží povinnosti odškodnění z 50 000 USD na 25 000 USD, vyjma jakýchkoli poplatků za nedodržení pravidel.

Článek 5 Důležité pravidelné ověření vašich systémů

K ověření stavu zařízení, systémů a/nebo sítí (a jejich součástí), které jsou vaše nebo vašich Franšízantů, a v nichž jsou uchovávány, zpracovávány nebo přenášeny Údaje držitelů karet nebo Citlivé ověřovací údaje, musíte podle PCI DSS každoročně a každých 90 dní, jak je popsáno níže, provést následující kroky.

K provedení ověření se požadují čtyři akce:

Akce 1: Zapojte se do Programu dodržování pravidel a zásad PCI společnosti American Express (dále jen „Program“) v souladu těmito pravidly.

Akce 2: Porozumějte vaší Úrovni obchodníka a Požadavkům na ověření.

Akce 3: Vyplňte Ověřovací dokumentaci, kterou musíte zaslat společnosti American Express.

Akce 4: Ověřovací dokumentaci zašlete společnosti American Express v předepsaných lhůtách.

Akce 1: Zapojte se do Programu dodržování pravidel a zásad společnosti American Express v souladu těmito Pravidly

Obchodníci na Úrovni 1, Obchodníci na Úrovni 2 a všichni Poskytovatelé služeb, jak jsou uvedeni níže, jsou povinni se zapojit do Programu v souladu s těmito pravidly. Společnost American Express může podle vlastního uvážení stanovit, že se určití Obchodníci na Úrovni 3 a Obchodníci na Úrovni 4 musí zúčastnit Programu v souladu s těmito pravidly.

Obchodníci a Poskytovatelé služeb, kteří se mají účastnit Programu, se musí v předepsaných lhůtách zaregistrovat na Portálu, který poskytuje Správce Programu vybraný společností American Express.

- Musí přijmout všechny přiměřené podmínky spojené s používáním Portálu.
- V rámci Portálu musíte přiřadit a poskytnout přesné informace alespoň o jednom kontaktu pro zabezpečení dat. Mezi požadované datové prvky patří:
  - jméno a příjmení
  - e-mailová adresa
  - telefonní číslo
  - poštovní doručovací adresa
- Při změně údajů je nutné uvést aktualizované nebo nové kontaktní údaje kontaktu přiděleného pro zabezpečení dat v rámci Portálu.
- Musíte zajistit, aby vaše systémy byly aktualizované a umožňovaly servisní komunikaci z vyhrazené domény Portálu.

Pokud neposkytnete nebo neaktualizujete kontaktní údaje pro zabezpečení dat, či neumožníte e-mailovou komunikaci, nijak se to neodrazí v našich právech na vyměření poplatků.

Akce 2: Porozumějte vaší Úrovni obchodníka a Požadavkům na ověření

Obchodníků se týkají čtyři Úrovně a Poskytovatelů služeb dvě Úrovně, které se zakládají na objemu Transakcí prostřednictvím Karet American Express.

- U Obchodníků se jedná o objem předložený jejich Provozovnami, který se shromažďuje na nejvyšší úrovni obchodnického účtu American Express.*
- U Poskytovatelů služeb se jedná o součet objemu předloženého Poskytovatelem služeb a Poskytovatelem služeb pro subjekty, kterým poskytujete služby.

Transakce pod názvem Platby iniciované kupujícím (BIP) nejsou pro stanovení Úrovně obchodníka a Požadavků na ověření zahrnuty do objemu transakcí prostřednictvím Karet American Express. Budete spadat do jedné z Úrovní obchodníků uvedených v tabulkách pro Obchodníky a Poskytovatele služeb níže.

* V případě Franšízantů toto zahrnuje objem z provozoven jejich Franšízorů. Franšízoři, kteří nařídí, aby jejich Franšízanti používali specifický systém Prodejního místa (POS) nebo Poskytovatele služeb, musí dotčeným Franšízantům rovněž poskytnout ověřovací dokumentaci.

Požadavky Obchodníka na ověřovací dokumentaci

Obchodníci (nikoli Poskytovatelé služeb) mají čtyři možné klasifikace Úrovně obchodníka. Po určení Úrovně obchodníka z níže uvedeného seznamu, viz Tabulka A-4: Ověřovací dokumentace obchodníka pro stanovení požadavků na ověřovací dokumentaci.

- **Obchodník na Úrovni 1** – nejméně 2,5 milionů Transakcí prostřednictvím Karty American Express ročně nebo jakýkoli Obchodník, kterého společnost American Express podle vlastního uvážení označí za Obchodníka na Úrovni 1.
- **Obchodník na Úrovni 2** – 50 000 až 2,5 milionů Transakcí prostřednictvím Karty American Express ročně.
- **Obchodník na Úrovni 3** – 10 000 až 50 000 Transakcí prostřednictvím Karty American Express ročně.
- **Obchodník na Úrovni 4** – méně než 10 000 Transakcí prostřednictvím Karty American Express ročně.

Tabulka A-4: Ověřovací dokumentace obchodníka

Úroveň obchodníka / Roční počet Transakcí American Express	Potvrzení o plnění požadavků pro Zprávu o plnění požadavků (ROC AOC)	Potvrzení o plnění požadavků pro Dotazník (SAQ AOC) A čtvrtletní externí skenování zranitelnosti sítě (Sken)	Potvrzení v programu STEP pro způsobilé Obchodníky
Úroveň 1/ 2,5 milionu nebo více	Povinné	Nelze aplikovat	Nepovinné se souhlasem společnosti American Express (nahrazuje ROC)
Úroveň 2/ 50 000 až 2,5 milionu	Nepovinné	Povinné SAQ AOC (pokud se nezasílá ROC AOC), pro určité typy SAQ je povinný sken	Povinné (nahrazuje SAQ a sken sítě nebo ROC)
Úroveň 3/ 10 000 až 50 000	Nepovinné	Nepovinné SAQ AOC (je však povinné, pokud je vyžadováno společností American Express), pro určité typy SAQ je povinný sken	Povinné (nahrazuje SAQ a sken sítě nebo ROC)
Úroveň 4/ 10 000 nebo méně	Nepovinné	Nepovinné SAQ AOC (je však povinné, pokud je vyžadováno společností American Express), pro určité typy SAQ je povinný sken	Povinné (nahrazuje SAQ a sken sítě nebo ROC)

* Aby se předešlo pochybnostem, Obchodníci na Úrovni 3 a 4 nemusejí předkládat Ověřovací dokumentaci, nevyžaduje-li to společnost American Express. Přesto musí dodržovat veškerá další ustanovení těchto Provozních pravidel zabezpečení dat a podléhají odpovědnosti podle těchto pravidel.

Společnost American Express si vyhrazuje právo prověřit úplnost,přesnost a vhodnost Ověřovací dokumentace PCI. Společnost American Express může požadovat, abyste k tomuto účelu předložili další podpůrné dokumenty k posouzení. Kromě toho má společnost American Express právo požadovat, abyste využili služeb QSA nebo PFI schválených Radou pro bezpečnostní standardy PCI.

Program vylepšení zabezpečovací technologie (STEP)

Obchodníci, kteří dodržují PCI DSS, se mohou podle uvážení společnosti American Express také kvalifikovat do programu STEP společnosti American Express, pokud ve svých prostředích pro zpracování Karet implementují určité další bezpečnostní technologie. STEP platí pouze v případě, kdy obchodník nezaznamenal Data incident v předchozích 12 měsících a pokud se 75 % všech obchodnických Transakcí prostřednictvím Karty provádí pomocí kombinace následujících možností zvýšeného zabezpečení.:

- **EMV, bezkontaktní EMV nebo digitální peněženka** – na aktivním Čipovém zařízení, které má platné a aktuální schválení/certifikaci EMVCo (www.emvco.com) a je schopné zpracovávat Transakce s Čipovými kartami v souladu s AEIPS. (Američtí obchodníci mají za povinnost zahrnout i bezkontaktní karty)
- **Point-to-Point šifrování (P2PE)** – komunikace se zpracovatelem Obchodníka pomocí systému Point-to-Point šifrování schváleného PCI-SSC nebo QSA
- **Tokenizace** – implementované tokenizační řešení musí:
  - splňovat specifikace EMVCo,
  - být zabezpečeno, zpracováváno, uchováváno, přenášeno a zcela spravováno poskytovatelem služeb třetí strany, který splňuje požadavky PCI, a
  - Token nesmí reverzním procesem odhalit Obchodníkovi nemaskovaná Čísla primárních účtů (PAN).

Pro obchodníky způsobilé pro program STEP jsou sníženy požadavky na Ověřovací dokumentaci PCI, jak je popsáno dále v části Akce 3: „Vyplňte Ověřovací dokumentaci, kterou musíte zaslat společnosti American Express“ níže.

Požadavky na Poskytovatele služeb

Poskytovatelé služeb (ne Obchodníci) mají dvě možné klasifikace Úrovně. Po určení Úrovně Poskytovatele služeb z níže uvedeného seznamu zjistěte v Tabulka A-5: Dokumentace Poskytovatele služeb požadavky na ověřovací dokumentaci.

Poskytovatel služeb na Úrovni 1 – nejméně 2,5 milionů Transakcí prostřednictvím Karty American Express ročně nebo jakýkoli Poskytovatel služeb, kterého společnost American Express považuje za Poskytovatele služeb na Úrovni 1.

Poskytovatel služeb na Úrovni 2 – méně než 2,5 milionů Transakcí prostřednictvím Karty American Express ročně nebo kterýkoli Poskytovatel služeb nepovažovaný společností American Express za Poskytovatele služeb na Úrovni 1.

Poskytovatelé služeb nejsou způsobilí pro program STEP.

Tabulka A-5: Dokumentace Poskytovatele služeb

Úroveň	Ověřovací dokumentace	Požadavek
1	Výroční Potvrzení o plnění požadavků pro Zprávu o plnění požadavků (ROC AOC)	Povinné
2	Výroční SAQ D (Poskytovatel služeb) a čtvrtletní sken sítě nebo Výroční Potvrzení o plnění požadavků pro Zprávu o plnění požadavků (ROC AOC), je-li to preferováno.	Povinné

Doporučuje se, aby Poskytovatelé služeb také dodržovali Dodatkové ověření entity určené PCI.

Akce 3: Vyplňte Ověřovací dokumentaci, kterou musíte zaslat společnosti American Express

Následující dokumenty jsou požadovány pro různé úrovně Obchodníků a Poskytovatelů služeb v souladu s výše uvedenými tabulkami pro Obchodníky a Poskytovatele služeb.

Pro příslušný typ hodnocení musíte předložit Potvrzení o plnění požadavků (AOC). AOC je prohlášením o stavu plnění požadavků a jako takové musí být podepsáno a opatřeno datem příslušnou úrovní vedení vaší organizace.

Kromě AOC může společnost American Express požadovat, abyste předložili kopii úplného hodnocení a podle našeho uvážení další podpůrné dokumenty prokazující soulad s požadavky PCI DSS. Tuto Ověřovací dokumentaci vyplníte na své náklady.

Potvrzení o plnění požadavků pro Zprávu o plnění požadavků (ROC AOC) – (každoroční požadavek) – Zpráva o plnění požadavků dokumentuje výsledky podrobné kontroly vašeho místního zařízení, systémů a sítí (a jejich součástí), kde jsou uchovávány, zpracovávány nebo přenášeny Údaje držitelů karet nebo Citlivé ověřovací údaje (nebo obojí). Existují dvě verze: jedna pro Obchodníky a druhá pro Poskytovatele služeb. Zprávu o dodržování pravidel musí provést:

- QSA, nebo
- vy a potvrdit váš výkonný ředitel, finanční ředitel, ředitel bezpečnosti IT nebo vedoucí oddělení

AOC musí být podepsat a datem opatřit QSA anebo interní bezpečnostní hodnotitel (ISA) a oprávněná úroveň vedení ve vaší organizaci a musí se společnosti American Express předložit alespoň jednou ročně.

Potvrzení o plnění požadavků pro Dotazník vlastního hodnocení (SAQ AOC) – **(každoroční požadavek)** – Dotazníky vlastního hodnocení pro vaše zařízení, systémy a sítě (a jejich součásti), kde jsou uchovávány, zpracovávány nebo přenášeny Údaje držitelů karet nebo Citlivé ověřovací údaje (nebo obojí). Existuje několik verzí dotazníku SAQ. Vyberte si jeden či více dotazníků podle prostředí, ve kterém se Prostředí údajů Držitelů karet.

Dotazníky SAQ mohou vyplňovat zaměstnanci vaší Společnosti, kteří jsou kvalifikováni k přesnému a důkladnému zodpovězení otázek, nebo si můžete na pomoc najmout QSA. AOC musí být podepsáno a opatřeno datem oprávněnou úrovní vedení ve vaší organizaci a musí být poskytnuto společnosti American Express alespoň jednou ročně.

Souhrnný přehled externího skenování zranitelností sítě od Schváleného dodavatele skenování (Sken ASV) – (90denní požadavek) – Externí skenování zranitelnosti je vzdálený test, který pomáhá identifikovat potenciální slabiny, zranitelnosti a chybné konfigurace internetových součástí Prostředí údajů Držitelů karet (např. webové stránky, aplikace, webové servery, poštovní servery, veřejně přístupné domény nebo hostitelé).

Sken ASV musí být proveden Schváleným dodavatelem skenování (ASV).

Pokud to vyžaduje SAQ, je třeba minimálně jednou za 90 dní předložit společnosti American Express Potvrzení o plnění požadavků skenování pro Zprávu o skenování ASV (AOSC) nebo shrnutí obsahující počet skenovaných cílů, potvrzení, že výsledky splňují postupy skenování PCI DSS, a stav potvrzení vyplněný ASV.

ROC AOC nebo STEP nemusí poskytovat shrnutí AOSC nebo Sken ASV, pokud o to není výslovně požádáno. V zájmu vyloučení pochybností je skenování povinné, pokud ho vyžaduje příslušný dotazník SAQ.

V zájmu vyloučení pochybností je ASV povinné, pokud ho vyžaduje příslušný dotazník SAQ.

Ověřovací dokumentace potvrzení programu STEP (STEP) – (každoroční požadavek) – STEP je k dispozici pouze pro Obchodníky, kteří splňují kritéria uvedená v Akce 2: „Porozumějte vaší Úrovni obchodníka a Požadavkům na ověření“ výše. Pokud vaše společnost splňuje podmínky, musíte každoročně vyplnit a odeslat společnosti American Express formulář Potvrzení v programu STEP. Formulář pro Potvrzení v programu STEP je k dispozici ke stažení na Portálu.

Nedodržení PCI DSS – (výroční, 90denní anebo ad hoc požadavek) – Pokud nedodržujete PCI DSS, musíte předložit jeden z následujících dokumentů:

- Potvrzení o plnění požadavků (AOC) včetně sekce „Část 4. Plán dalších akcí v případě neplnění požadavků“ (ke stažení na webových stránkách Rady pro bezpečnostní standardy PCI)
- Shrnutí nástroje PCI s prioritním přístupem (ke stažení na webových stránkách Rady pro bezpečnostní standardy PCI)
- Šablonu plánu projektu (k dispozici ke stažení na zabezpečeném portálu společnosti SecureTrust). Plán projektu lze předložit namísto výročního potvrzení (SAQ/ROC) a/nebo namísto požadavku na skenování.

Každý z výše uvedených dokumentů musí obsahovat stanovené datum nápravy maximálně do dvanácti (12) měsíců od data vypracování dokumentu, aby bylo dosaženo souladu s pravidly. Společnosti American Express pak musíte poskytovat pravidelné aktualizace o postupu k nápravě vašeho stavu nedodržování pravidel (Obchodníci na Úrovni 1, Úrovni 2, Úrovni 3 a Úrovni 4 a všichni Poskytovatelé služeb). Nápravná opatření nezbytná k dosažení souladu s PCI DSS se musí vypořádat na vaše náklady.

Nápravná opatření nezbytná k dosažení souladu s PCI DSS se musí vypořádat na vaše náklady.

Společnost American Express vám nebude účtovat poplatky za neověření (popsané níže) při neplnění požadavků předcházejícím stanovené datum nápravy, nadále však ponesete vůči společnosti American Express odpovědnost za veškeré povinnosti odškodnění za Data incidenty a budou pro vás platit všechna ostatní ustanovení těchto pravidel.

Aby se předešlo všem pochybnostem, upozorňujeme, že Obchodníci, kteří nedodržují PCI DSS, nejsou způsobilí pro program STEP.

Akce 4: Ověřovací dokumentaci zašlete společnosti American Express

Všichni Obchodníci a Poskytovatelé služeb, od nichž se požaduje účast v Programu, musí předložit Ověřovací dokumentaci označenou jako „povinnou“ v tabulkách v Akce 2: „Porozumějte vaší Úrovni obchodníka a Požadavkům na ověření“ společnosti American Express v souladu s platnými termíny.

Ověřovací dokumentaci musíte společnosti American Express předložit prostřednictvím Portálu, který poskytuje Správce Programu vybraný společností American Express. Předložením Ověřovací dokumentace prohlašujete a zaručujete společnosti American Express, že následující skutečnosti jsou pravdivé (podle vašich nejlepších schopností):

- vaše hodnocení bylo úplné a důkladné,
- stav PCI DSS je přesně znázorněn v době vyplnění, ať už je v souladu, či nikoli,
- jste oprávněni zveřejnit informace v něm obsažené a poskytujete Ověřovací dokumentaci společnosti American Express, aniž byste porušili práva jakékoli jiné strany.

Poplatky za neověření a Předčasné ukončení Smlouvy

Společnost American Express má právo účtovat vám poplatky za neověření a předčasně ukončit tuto Smlouvu, jestliže nesplníte tyto požadavky či neposkytnete společnosti American Express do příslušného termínu povinnou Ověřovací dokumentaci. Společnost American Express vás samostatně upozorní na příslušné termíny pro každé roční a čtvrtletní období.

Tabulka A-6: Poplatky za neověření

Popis*	Obchodník na Úrovni 1 nebo Poskytovatel služeb na Úrovni 1	Obchodník na Úrovni 2 nebo Poskytovatel služeb na Úrovni 2	Obchodník na Úrovni 3 nebo na Úrovni 4
Bude účtován poplatek za neověření, jestliže Ověřovací dokumentace není obdržena do prvního termínu.	25 000 USD	5 000 USD	50 USD
Pokud nebude Ověřovací dokumentace doručena do druhého termínu, bude vyměřen dodatečný poplatek za neověření.	35 000 USD	10 000 USD	100 USD
Pokud nebude Ověřovací dokumentace doručenado třetího termínu, bude vyměřen dodatečný poplatek za neověření. **POZNÁMKA:** Poplatky za neověření se budou uplatňovat až do předložení Ověřovací dokumentace.	45 000 USD	15 000 USD	250 USD

* Poplatky za neověření budou stanoveny v ekvivalentu místní měny.

* Neplatí pro Argentinu.

Pokud nebudou splněny vaše povinnosti týkající se Ověřovací dokumentace PCI DSS, má společnost American Express právo kumulativně uložit poplatky za neověření, zadržet platby a/nebo ukončit smlouvu.

Článek 6 Ochrana důvěrných informací

Společnost American Express přijme přiměřená opatření (a zajistí, aby přiměřená opatření přijali i její zmocněnci a subdodavatelé, včetně Poskytovatele Portálu) k ochraně důvěrného charakteru vašich zpráv o dodržování pravidel, včetně Ověřovací dokumentace, a nezpřístupní Ověřovací dokumentaci jakékoli třetí straně (kromě Přidružených společností, zmocněnců či zástupců společnosti American Express, Poskytovatelů služeb a subdodavatelů) po dobu tří let od obdržení této dokumentace, kromě případů, kdy tato povinnost ochrany důvěrných informací neplatí pro Ověřovací dokumentaci představující údaje, které:

a. jsou společnosti American Express známé již před zpřístupněním;

b. jsou nebo se stanou veřejně známými, aniž by společnost American Express porušila ustanovení tohoto odstavce;

c. byly společností American Express legálně získány od třetí strany bez povinnosti ochrany důvěrných informací;

d. jsou nezávisle vyvinuty společností American Express; nebo

e. jejich zpřístupnění se vyžaduje nařízením soudu, administrativních nebo vládních orgánů či jakýmkoli zákonem, pravidlem nebo předpisem, předvoláním, žádostí o zjištění či jiným administrativním nebo právním postupem, či jakýmkoli formálním nebo neformálním vyšetřováním jakéhokoli vládního orgánu či vládní instituce (včetně regulatorních orgánů, inspektorů, vyšetřovatelů nebo policejních orgánů).

Článek 7 Vyloučení odpovědnosti

SPOLEČNOST AMERICAN EXPRESS SE TÍMTO ZŘÍKÁ JAKÝCHKOLI PROHLÁŠENÍ, ZÁRUK A ODPOVĚDNOSTI SPOJENÝCH S TĚMITO PROVOZNÍMI PRAVIDLY ZABEZPEČENÍ ÚDAJŮ, PCI DSS, TECHNICKÝCH ÚDAJŮ EMV A KLASIFIKACÍ A VÝSLEDKŮ QSA, ASV NEBO PFI (NEBO KTERÝCHKOLI Z NICH), AŤ UŽ VÝSLOVNÝCH, NÁSLEDNÝCH, ZE ZÁKONA ČI JINÝCH, VČETNĚ ZÁRUK PRODEJNOSTI ČI VHODNOSTI PRO URČITÝ ÚČEL.

VYDAVATELÉ KARET AMERICAN EXPRESS NEJSOU PODLE TĚCHTO ZÁSAD OPRÁVNĚNÝMI TŘETÍMI STRANAMI.

Užitečné webové stránky

Zabezpečení dat společnosti American Express: www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC: www.pcisecuritystandards.org

Glosář

Pouze pro účely tohoto dokumentu Provozní pravidla zabezpečení dat (DSOP) platí následující definice, které budou mít přednost v případě rozporu s pojmy uvedenými v dokumentu *Předpisy pro obchodníky*.

Citlivé ověřovací údaje mají význam uvedený v aktuálním Glosáři pro PCI DSS.

Čip znamená integrovaný mikročip na Kartě obsahující informace o Držiteli karty a informace o účtu.

Čipová karta znamená Kartu, která obsahuje Čip a která může vyžadovat kód PIN k ověření identity Držitele karty či informací o účtu uvedených na Čipu, nebo obou (někdy v našich materiálech označována jako tzv. inteligentní karta, Karta EMV či ICC nebo karta s integrovanými obvody).

Čipové zařízení znamená platební zařízení v prodejním místě s platným a aktuálním oprávněním/certifikací EMVCo (www.emvco.com) schopné zpracovat Transakce s Čipovými kartami v souladu s AEIPS.

Číslo karty znamená jedinečné identifikační číslo, které Vydavatel přiděluje Kartě při jejím vydání.

Číslo primárního účtu nebo PAN (Primary Account Number) má význam uvedený v aktuálním slovníku pojmů pro PCI DSS.

Číslo zneužité karty znamená číslo účtu Karty American Express spojené s Data incidentem.

Data incident znamená incident týkající se zneužití nebo podezření na zneužití šifrovacích klíčů společnosti American Express anebo nejméně jednoho čísla účtu Karty American Express, při kterém dojde:

- k neoprávněnému přístupu či použití Šifrovacích klíčů, Údajů držitelů karet či Citlivých ověřovacích údajů (nebo jejich kombinací) uložených, zpracovávaných nebo přenášených na zařízeních, systémech či sítích (nebo jejich součástech), které jsou vaše nebo které spravujete nebo ke kterým poskytujete přístup;
- k použití takových Šifrovacích klíčů, Údajů držitelů karet či Citlivých ověřovacích údajů (nebo jejich kombinací) jinak než v souladu se Smlouvou; a/nebo
- k podezření či potvrzení, že došlo ke ztrátě, krádeži nebo neoprávněnému přisvojení jakýchkoli prostředků, materiálů, záznamů nebo informací obsahujících takové Šifrovací klíče, Údaje držitelů karet či Citlivé ověřovací údaje (nebo jejich kombinaci).

Den upozornění znamená datum, kdy společnost American Express poskytne vydavatelům konečné oznámení o Data incidentu. Takové datum závisí na obdržení závěrečné forenzní zprávy nebo interní analýzy ze strany společnosti American Express a bude stanoveno podle uvážení společnosti American Express.

Dotazník vlastního hodnocení nebo SAQ (Self-Assessment Questionnaire) znamená nástroj pro vlastní vyhodnocení vytvořený institucí Payment Card Industry Security Standards Council, LLC, a určený k vyhodnocení a potvrzení dodržování PCI DSS.

Držitel karty znamená jednotlivce či entitu, (i) kteří s vydavatelem uzavřeli dohodu o otevření účtu spojeného s Kartou, nebo (ii) jejichž jméno je uvedeno na Kartě.

Forenzní vyšetřovatel PCI nebo PFI (PCI Forensic Investigator) znamená entitu, která byla schválena institucí Payment Card Industry Security Standards Council, LLC k provádění forenzních šetření porušení nebo zneužití Údajů platebních karet.

Franšízant znamená nezávisle vlastněnou a provozovanou třetí stranu (včetně franšízanta, držitele licence nebo pobočky), jinou než Přidruženou společnost, která je držitelem licence udělené Franšízorem k provozování

franšízy a která uzavřela s Franšízorem písemnou dohodu, podle které trvale ukazuje externí označení totožnosti výrazně zobrazující Značky Franšízora nebo se veřejně prezentuje jako člen skupiny společností Franšízora.

Franšízor znamená provozovatele podniku, který uděluje licenci osobám nebo entitám (Franšízantům) k distribuci zboží a/nebo služeb pod značkou provozovatele nebo k provozování podniku s použitím značky provozovatele; poskytuje Franšízantům asistenci při provozování jejich provozoven nebo ovlivňuje způsob tohoto provozování; a vyžaduje ze strany Franšízanta zaplacení poplatku.

Informace o držiteli karty znamená informace o Držitelích karty American Express a Transakcích Karty, včetně jmen, adres, čísel účtů karet a identifikačních čísel karet (CID).

Karta American Express nebo **Karta** znamená jakoukoli kartu, zařízení pro přístup na účet nebo platební zařízení či platební službu se jménem, logem, ochrannou známkou, značkou služeb, obchodním názvem nebo jiným výlučným designem či popisem společnosti American Express nebo jejích přidružených společností a vydanou vydavatelem, nebo číslo účtu karty.

Kredit znamená částku Platby, kterou Držiteli karty vrátíte za nákupy či platby prostřednictvím Karty.

Kryté strany znamenají všechny vaše zaměstnance, zmocněnce, zástupce, subdodavatele, Zpracovatele, Poskytovatele služeb, poskytovatele platebních zařízení v prodejních místech (POS) nebo systémů a platebních řešení, Entity spojené s vaším Obchodnickým účtem American Express a všechny strany, kterým můžete poskytovat přístup k Informacím o držitelích karet v souladu s touto Smlouvou.

Kvalifikovaný expert na zabezpečení nebo QSA (Qualified Security Assessor) znamená entitu, která byla institucí Payment Card Industry Security Standards Council, LLC schválena k ověřování plnění požadavků PCI DSS.

Norma pro zabezpečení údajů platebních karet nebo PCI DSS (Payment Card Industry Data Security Standard) znamená oborovou normu, která je k dispozici na adrese www.pcisecuritystandards.org.

Obchodník znamená obchodníka a veškeré jeho přidružené společnosti, které přijímají Karty American Express podle Smlouvy se společností American Express nebo některou z jejích přidružených společností.

Obchodník na Úrovni 1 znamená Obchodníka s nejméně 2,5 miliony Transakcí prostřednictvím Karty American Express ročně nebo kteréhokoli Obchodníka považovaného společností American Express za Obchodníka na Úrovni 1.

Obchodník na Úrovni 2 znamená Obchodníka s 50 000 až 2,5 miliony Transakcí prostřednictvím Karty American Express ročně.

Obchodník na Úrovni 3 znamená Obchodníka s 10 000 až 50 000 Transakcí prostřednictvím Karty American Express ročně.

Obchodník na Úrovni 4 znamená Obchodníka s méně než 10 000 Transakcí prostřednictvím Karty American Express ročně.

Období data incidentu znamená období vniknutí (nebo podobně určené časové období) uvedené v závěrečné forenzní zprávě (např. zprávě PFI), nebo pokud není známo, až 365 dní před posledním Dnem upozornění čísel potenciálně Zneužitých karet zapojených do kompromitace dat, která nám byla nahlášena.

Ověřovací dokumentace znamená dokumenty AOC připravené ve spojení s Výročním hodnocením zabezpečení místa nebo SAQ, AOSC a shrnutí zjištění ve spojení s Čtvrtletními skeny sítě nebo Výročním potvrzením Programu vylepšení zabezpečovací technologie.

PCI DSS znamená oborovou normu pro zabezpečení údajů platebních karet (Payment Card Industry Data Security Standard), která je k dispozici na adrese www.pcisecuritystandards.org.

Platba znamená platbu či koupi pomocí Karty.

Platební aplikace má význam uvedený v aktuálním Glosáři k Oborové normě pro bezpečný software a Oborové normě pro životní cyklus bezpečného softwaru, který je k dispozici na www.pcisecuritystandards.org.

Point to Point šifrování (P2PE) znamená řešení, které kryptograficky chrání údaje účtu od okamžiku, kdy obchodník přijme platební kartu do zabezpečeného místa dešifrování.

Portál znamená systém pro podávání zpráv poskytovaný správcem Programu PCI společnosti American Express vybraným společností American Express. Obchodníci a poskytovatelé služeb jsou povinni používat Portál k předkládání ověřovací dokumentace PCI společnosti American Express.

Potvrzení o plnění požadavků nebo AOC (Attestation of Compliance) znamená prohlášení o stavu vašeho dodržování PCI DSS na formuláři poskytnutém institucí Payment Card Industry Security Standards Council, LLC.

Poskytovatelé služeb znamenají schválené zpracovatele, zpracovatele třetích stran, poskytovatele spojení, integrátory POS systémů a veškeré další poskytovatele systémů POS nebo dalších řešení nebo služeb zpracovávání plateb pro Obchodníky.

Poskytovatel služeb na Úrovni 1 znamená Poskytovatele služeb s nejméně 2,5 miliony Transakcí prostřednictvím Karty American Express ročně nebo kteréhokoli Poskytovatele služeb považovaného společností American Express za Poskytovatele služeb na Úrovni 1.

Poskytovatel služeb na Úrovni 2 znamená Poskytovatele služeb s méně než 2,5 miliony Transakcí prostřednictvím Karty American Express ročně nebo kteréhokoli Poskytovatele služeb nepovažovaného společností American Express za Poskytovatele služeb na Úrovni 1.

Potvrzení o plnění požadavků skenování nebo AOSC (Attestation of Scan Compliance) znamená prohlášení o stavu vašeho dodržování PCI DSS na základě skenu sítě na formuláři poskytnutém institucí Payment Card Industry Security Standards Council, LLC.

Požadavky instituce Payment Card Industry Security Standards Council (PCI SSC) představují sadu norem a požadavků týkajících se zabezpečení a ochrany údajů souvisejících s platebními kartami, včetně PCI DSS a PA DSS. Jsou k dispozici na adrese www.pcisecuritystandards.org.

Program cílené analýzy nebo TAP (Targeted Analysis Programme) znamená program, který poskytuje časnou identifikaci potenciálního zneužití údajů Držitelů karet ve vašem Prostředí údajů Držitelů karet (CDE). Viz Článek 1, „Program cílené analýzy (TAP)“.

Program vylepšení zabezpečovací technologie (STEP) představuje program společnosti American Express, ve kterém jsou Obchodníci motivováni k nasazování technologií zlepšujících zabezpečení dat.

Program znamená Program shody s PCI společnosti American Express.

Prostředí údajů Držitelů karet nebo CDE (Cardholder Data Environment) znamená osoby, procesy a technologii ukládající, zpracovávající nebo převádějící údaje držitelů karet nebo citlivé ověřovací údaje.

Schválené PCI znamená, že Zařízení pro zadání kódu PIN nebo Platební aplikace (či obojí) je v době použití na seznamu schválených společností a poskytovatelů instituce PCI Security Standards Council, LLC, který je k dispozici na adrese www.pcisecuritystandards.org.

Schválené řešení Point-to-Point šifrování (P2PE), zahrnuto do seznamu ověřených řešení PCI SSC nebo ověřených P2PE společností Kvalifikovaného experta na zabezpečení PCI SSC.

Schválený dodavatel skenování nebo ASV (Approved Scanning Vendor) znamená Entitu, která byla institucí Payment Card Industry Security Standards Council, LLC schválena k ověřování plnění určitých požadavků PCI DSS prostřednictvím skenování zranitelnosti rozhraní spojených s internetem.

Systém Prodejního místa nebo POS (Point of Sale) znamená systém či zařízení ke zpracování informací, včetně terminálu, počítače, elektronické pokladny, bezkontaktní čtečky, platebního nástroje či procesu, používané Obchodníkem k získání schválení nebo ke sběru údajů o Transakcích, či obojímu.

Šablona závěrečné forenzní zprávy o incidentu je šablona dostupná u Rady pro bezpečnostní standardy PCI, která je k dispozici na adrese www.pcisecuritystandards.org.

Šifrovací klíč (šifrovací klíč American Express) znamená všechny klíče používané při zpracování, tvorbě, načítání a/nebo ochraně údajů o účtu. Toto zahrnuje mimo jiné následující:

- Hlavní šifrovací klíče: Zone Master Keys (ZMK, Hlavní klíče zóny) a Zone Pin Keys (ZPK, Klíče zóny pro kódy PIN)
- Hlavní klíče používané v zabezpečených kryptografických zařízeních: Local Master Keys (LMK, Místní hlavní klíče)
- Card Security Code Keys (CSCK, Klíče zabezpečení kódů karet)
- Klíče kódů PIN: Base Derivation Keys (BDK, Základní derivační klíče), PIN Encryption Key (PEK, Klíče šifrování kódů PIN) a ZPK

Specifikace EMV znamená specifikace vydané společností EMVCo, LLC, které jsou k dispozici na adrese www.emvco.com.

Technologie snižování rizik znamená technologická řešení, která zvyšují zabezpečení Údajů držitelů karet American Express a Citlivých ověřovacích údajů, jak stanoví společnost American Express. Chcete-li splnit kritéria pro určení Technologie snižování rizik, musíte prokázat efektivní využití technologie v souladu s její klasifikací a zamýšleným účelem. Mezi příklady patří mimo jiné: EMV, Point-to-Point šifrování a tokenizace.

Token znamená kryptografický token, který nahrazuje PAN na základě daného indexu za nepředvídatelnou hodnotu.

Transakce znamená Platbu nebo Kredit realizovaní prostřednictvím Karty.

Transakce EMV znamená transakci prostřednictvím karty s integrovaným obvodem (někdy také označované jako IC Karta, čipová karta, inteligentní karta, karta EMV nebo ICC), kterou lze používat pro platby v místech s terminálem POS s platným a aktuálním schválením typu EMV. Schválení typu EMV jsou k dispozici na adrese www.emvco.com.

Transakce typu Platby iniciované kupujícím nebo BIP (Buyer Initiated Payment) znamenají platební transakce umožněné prostřednictvím souboru platebního příkazu, zpracovaného v systému BIP.

Údaje držitelů karet mají význam uvedený v aktuálním Glosáři pro PCI DSS.

Úroveň obchodníka znamená označení, které přidělujeme obchodníkům v souvislosti s jejich povinností ověření shody s PCI DSS, jak je popsáno v Článku 5, „Důležité pravidelné ověření vašich systémů“.

Vydavatel znamená jakoukoli Entitu (včetně společnosti American Express a jejích Přidružených společností), které společnost American Express nebo některá její Přidružená společnost udělila licenci k vydávání Karet a k provozování obchodní činnosti spočívající ve vydávání Karet.

Zabezpečovací požadavky PCI pro kódy PIN znamenají oborové požadavky na zabezpečení kódů PIN pro platební karty, které jsou k dispozici na adrese www.pcisecuritystandards.org.

Zařízení pro zadání kódu PIN má význam uvedený v aktuálním Glosáři termínů pro transakce platebními kartami s kódy PIN (PTS) prostřednictvím platebních míst (POI), požadavky na modulární zabezpečení, který je k dispozici na adrese www.pcisecuritystandards.org.

Zpracovatel znamená poskytovatele služeb Obchodníkům, který umožňuje schválení a předložení ke zpracování do sítě American Express.