

Provozní pravidla zabezpečení dat (DSOP)

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 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 4, „Důležité pravidelné ověření vašich systémů“](#), pokud není v tomto článku stanoveno jinak).

Článek 2 Povinnosti spojené s Data incidenty

Jakýkoliv Data incident musíte okamžitě oznámit společnosti American Express, v každém případě nejpozději dvacet čtyři (24) 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 předčísli 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 2, „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 2, „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 American Express, Vydavatelům, ostatním účastníkům v Síti American Express a veřejnosti v rozsahu vyžadovaném Příslušnými právními předpisy, soudními, administrativními či regulačními 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 3 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 3, „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 3, „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 tohoto [Článku 3. „Odškodnění v případě Data incidentu“](#),
 - v době Data incidentu jste dodržovali PCI DSS (což je potvrzeno vyšetřováním Data incidentu Forezním 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 3. „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 2. „Povinnosti spojené s Data incidenty“](#). Aby se předešlo pochybnostem, upozorňujeme, že celkový poplatek za nedodržení pravidel v oblasti Data incidentů, stanový 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 náúčtovat na váš bankovní Účet).

Povinnosti Obchodníků 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 snižování 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),
- forezní 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:

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 Forezním 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 určení 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 Forezním vyšetřovatelem PFI.
- Snížení povinnosti odškodnění se nevztahuje na žádné poplatky za nedodržení pravidel splatné v souvislosti s Data incidentem.

Př.	Použití Technologí snižování rizik	Způsobilost pro rozšířené snížení povinnosti odškodnění?	Snížení
1	80 % Transakcí zpracováno na Čipových zařízeních 0 % lokalit používá jinou Technologii snižování rizik	Ne	50 %: Standardní snížení (méně než 75% použití Technologí snižování rizik nestačí na splnění kritérií pro Rozšířené snížení) ¹
2	80 % Transakcí zpracováno na Čipových zařízeních 77 % lokalit používá jinou Technologii snižování rizik	Ano	77 %: Rozšířené snížení (na základě 77% použití Technologie snižování rizik)
3	93 % Transakcí zpracováno na Čipových zařízeních 100 % lokalit používá jinou Technologii snižování rizik	Ano	93 %: Rozšířené snížení (na základě zpracování 93 % Transakcí na Čipových zařízeních)
4	40 % Transakcí zpracováno na Čipových zařízeních 90 % lokalit používá jinou Technologii snižování rizik	Ne	50 %: Standardní snížení (méně než 75 % Transakcí na Čipových zařízeních nestačí na splnění kritérií pro Rozšířené snížení)

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 4 Důležité pravidelné ověření vašich systémů

V souladu s PCI DSS musíte podniknout, jak je popsáno níže, následující akce ke každoročnímu a čtvrtletnímu ověření stavu zařízení, systémů a/nebo sítí (a jejich součástí), které jsou vaše nebo vašeho Franšízanta, a na kterých jsou ukládány, zpracovávány či přenášeny Údaje držitelů karet nebo Citlivé ověřovací údaje.

K provedení ověření se požadují čtyři akce:

[Akce 1:](#) Zapojte se do Programu dodržování pravidel a zásad společnosti American Express v souladu těmito Pravidly.

[Akce 2:](#) Porozumějte vaší Úrovní 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 pro dodržování pravidel a zásad PCI společnosti American Express v souladu s těmito pravidly poskytnutím celého jména, e-mailové adresy, telefonního čísla a poštovní adresy jednotlivce, který bude jejich kontaktní osobou pro záležitosti týkající se zabezpečení údajů. Tyto informace jste povinni dodat společnosti SecureTrust, divizi společnosti Trustwave (<https://portal.securetrust.com>), která tento program pro společnost American Express spravuje, a to jedním ze způsobů uvedených dále v části [Akce 4: „Ověřovací dokumentaci zašlete společnosti American Express“](#). Jestliže se tyto informace změní, musíte o tom společnost SecureTrust informovat a poskytnout jí aktualizované informace. Pokud tyto kontaktní informace neposkytnete, nijak to neovlivní naše právo účtovat poplatky za neověření, jak je stanoveno v [Tabulce poplatků za neověření](#).

Společnost American Express může podle vlastního uvážení stanovit, že se určití Obchodníci na úrovni 3 a Obchodníci na úrovni 4 musí zúčastnit Programu dodržování zásad a pravidel společnosti American Express v souladu těmito pravidly. V takovém případě jim zašle písemné upozornění. Tito Obchodníci se v takovém případě musí do programu zařadit nejpozději do 90 dnů od obdržení takového upozornění.

Akce 2: Porozumějte vaší Úrovní a Požadavkům na ověření

Obchodníků se týkají čtyři Úrovně a Poskytovatelů služeb dvě Úrovně, které se zakládají na objemu Transakcí prostřednictvím Karet American Express. Pro Obchodníky se jedná o objem předložený jejich provozovny, který se shromažďuje na nejvyšší úrovni obchodnického účtu American Express.* Budete spadat do jedné z Úrovní uvedených v tabulkách pro Obchodníky, respektive Poskytovatele služeb, jak je uvedeno níže. Transakce pod názvem Platby iniciované kupujícím (BIP) nejsou pro stanovení Úrovně obchodníka a požadavků na ověření zahrnuty do objemu transakcí prostřednictvím Karet American Express.

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

Požadavky pro Obchodníky

Obchodníci (ne Poskytovatelé služeb) mají čtyři možné klasifikace úrovně a požadavků na ověření. Po určení úrovně Obchodníka podle níže uvedeného seznamu v Tabulce Obchodníků zjistíte požadavky na ověřovací dokumenty.

- **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 Obchodníků

Úroveň obchodníka / Roční počet Transakcí American Express	Ověřovací dokumentace		
	Zpráva o kontrole dodržování pravidel v daném místě (ROC)	Dotazník vlastního hodnocení (SAQ) A TAKÉ čtvrtletní skeny sítě	Potvrzení v programu STEP pro způsobilé Obchodníky
Úroveň 1/ 2,5 milionu nebo více	Povinné	Nelze aplikovat	Nepovinné (nahrazuje ROC)
Úroveň 2/ 50 000 až 2,5 milionu	Nepovinné	Povinný SAQ (pokud se nezasílá Zpráva o kontrole zabezpečení místa); pro určité typy SAQ je povinný sken	Povinné (nahrazuje SAQ a sken sítě nebo ROC)
Úroveň 3/ 10 000 až 50 000	Nepovinné	Nepovinný SAQ (je však povinný, pokud jej vyžaduje společnost American Express); pro určité typy SAQ je povinný sken	Povinné (nahrazuje SAQ a sken sítě nebo ROC)
Úroveň 4/ 10 000 nebo méně	Nepovinné	Nepovinný SAQ (je však povinný, pokud jej vyžaduje společnost 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, nevžaduje-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 přesnost a vhodnost ověřovací dokumentace PCI podle potřeby, včetně toho, že na náklady společnosti American Express zapojí experta QSA nebo Forezního vyšetřovatele PFI dle našeho výběru.

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 případech, kdy obchodník nezaznamenal Data incident v předchozích 12 měsících a pokud se 75 % všech obchodnických Transakcí prostřednictvím Karty provádí pomocí:

- **EMV** – aktivního Čipového zařízení s platným a aktuálním oprávněním/certifikací EMVCo (www.emvco.com), schopného zpracovat 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.

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“](#).

Požadavky na Poskytovatele služeb

Poskytovatelé služeb (ne Obchodníci) mají dvě možné klasifikace úrovně a požadavků na ověření. Po určení úrovně Poskytovatele služeb podle níže uvedeného seznamu zjistíte v Tabulce Poskytovatelů 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 Poskytovatelů služeb

Úroveň	Ověřovací dokumentace	Požadavek
1	Výroční zpráva o kontrole zabezpečení místa v souladu s pravidly	Povinné
2	Výroční SAQ D (Poskytovatel služeb) a čtvrtletní sken sítě nebo Výroční zpráva o kontrole zabezpečení místa v souladu s pravidly, 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 Obchodníků a Poskytovatelů služeb.

Výroční hodnocení zabezpečení místa – Jedná se o podrobnou každoroční kontrolu vašeho zařízení, vašich systémů a sítí (včetně jejich součástí), kde se ukládají, zpracovávají nebo přenášejí Údaje držitelů karet nebo Citlivé ověřovací údaje (nebo obojí). Hodnocení musí provést:

- expert QSA, nebo
- vy, a takové hodnocení musí být potvrzeno vaším generálním ředitelem, finančním ředitelem, ředitelem pro zabezpečení informací nebo vedoucím společnosti, a musí být společnosti American Express předloženo jako součást příslušného Potvrzení o plnění požadavků (AOC).

Potvrzení AOC musí prokázat dodržení všech požadavků PCI DSS a na požádání zahrnout kopie úplného textu zpráv o dodržování pravidel (Obchodníci na úrovni 1 a Poskytovatelé služeb na úrovni 1).

Výroční dotazník vlastního hodnocení – Výroční vlastní hodnocení je proces využívající Dotazník vlastního hodnocení PCI DSS (SAQ), který umožňuje vlastní kontrolu vašeho zařízení, vašich systémů a sítí (včetně jejich součástí), kde se ukládají, zpracovávají nebo přenášejí Údaje držitelů karet nebo Citlivé ověřovací údaje (nebo obojí). Výroční vlastní hodnocení musíte provést vy a potvrdit je musí váš generální ředitel, finanční ředitel, ředitel pro zabezpečení informací nebo vedoucí společnosti. Část AOC z dotazníku SAQ musí být každý rok zaslána společnosti American Express. Část AOC z dotazníku SAQ musí potvrzovat, že splňujete všechny požadavky PCI DSS, a na požádání zahrnout úplné kopie SAQ (Obchodníci na úrovni 2, Obchodníci na úrovni 3, Obchodníci na úrovni 4, Poskytovatelé služeb na úrovni 2).

Čtvrtletní sken sítě – Jde o proces, který dálkově testuje vaše počítačové sítě připojené k internetu a webové servery z hlediska známek možných slabých a zranitelných míst. Musí jej provádět Schválený dodavatel skenování (**ASV**). Každého čtvrt roku musíte vyplnit a zaslat společnosti American Express Skenovací zprávu vydanou ASV jako Potvrzení o plnění požadavků skenování (**AOSC**) nebo shrnutí s výsledky skenu (a na požádání celé kopie skenu). AOSC nebo shrnutí musí potvrzovat, že výsledky splňují skenovací postupy PCI DSS, že nebyly zjištěny žádné vysoce rizikové položky a že sken je úspěšný či splňuje podmínky (všichni Obchodníci kromě těch, kteří rovněž předloží Zprávu o kontrole zabezpečení místa, Obchodníků způsobilých pro STEP a všech Poskytovatelů služeb). Aby se předešlo pochybnostem, upozorňujeme, že Čtvrtletní skeny sítě jsou povinné, pokud to vyžaduje příslušný dotazník SAQ.

Ověřovací dokumentace Výročního potvrzení programu STEP – Výroční potvrzení kvalifikace STEP společnosti American Express („Potvrzení STEP“) je dostupné pouze Obchodníkům, kteří splňují kritéria uvedená v části [Akce 2: „Porozumějte vaší Úrovni a Požadavkům na ověření“](#). Potvrzení STEP zahrnuje proces s použitím požadavků PCI DSS, který umožňuje vlastní kontrolu vašeho zařízení, systémů a sítí (včetně jejich součástí),

kde se ukládají, zpracovávají nebo přenášejí Údaje držitelů karet nebo Citlivé ověřovací údaje (nebo obojí). Výroční vlastní hodnocení musíte provést vy a potvrdit je musí váš generální ředitel, finanční ředitel, ředitel pro zabezpečení informací nebo vedoucí společnosti. Tento proces musíte dokončit každoročním odesláním formuláře Potvrzení STEP společnosti American Express. (Pouze Obchodníci způsobilí pro STEP.) Formulář Výročního potvrzení programu STEP je k dispozici ke stažení na zabezpečeném portálu společnosti SecureTrust.

Shrnutí plnění požadavků („SOC“) – Dokument, jehož prostřednictvím může Franšízor nebo Poskytovatel služeb nahlásit stav souladu s PCI svých Franšízantů. Šablona SOC je k dispozici ke stažení na zabezpečeném portálu společnosti SecureTrust.

Nedodržení PCI DSS – Jestliže nesplňujete požadavky PCI DSS, musíte předložit jeden z následujících dokumentů:

- Potvrzení o plnění požadavků (AOC) včetně sekce „Část 4. Plán dalších akcí v případě neplnění požadavků“
- Shrnutí nástroje PCI s prioritním přístupem a Potvrzení o plnění požadavků (PASAOC)
- Šablonu plánu projektu (k dispozici ke stažení na zabezpečeném portálu společnosti SecureTrust)

Každý z výše uvedených dokumentů musí obsahovat stanovené datum nápravy maximálně do 12 měsíců od data vypracování dokumentu, aby bylo dosaženo souladu s pravidly. Příslušné dokumenty jste povinni dodat společnosti American Express, a to jedním ze způsobů uvedených níže v části [Akce 4: „Ověřovací dokumentaci zašlete společnosti American Express“](#). 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). Aby se předešlo všem pochybnostem, upozorňujeme, že Obchodníci, kteří nedodržují PCI DSS, nejsou způsobilí pro program STEP. Společnost American Express vám nebude účtovat poplatky za neověření (popsané níže) při neplnění požadavků před stanoveným datem nápravy, nadále však ponese vůči společnosti American Express odpovědnost za veškeré povinnosti odškodnění za Data incidenty a budou pro vás platit všechna ostatní ustanovení těchto pravidel.

Akce 4: Ověřovací dokumentaci zašlete společnosti American Express

Všichni Obchodníci a Poskytovatelé služeb, od nichž se požaduje účast v Programu dodržování pravidel a zásad PCI společnosti American Express, musí předložit Ověřovací dokumentaci označenou jako povinnou v tabulce v části [Akce 2: „Porozumějte vaší Úrovni a Požadavkům na ověření“](#). Ověřovací dokumentaci musíte zaslat společnosti SecureTrust jedním z následujících způsobů:

- **Zabezpečený portál:** Ověřovací dokumentace může být nahrána prostřednictvím zabezpečeného portálu společnosti SecureTrust na <https://portal.securetrust.com>. Pokyny k používání tohoto portálu si můžete vyžádat od společnosti SecureTrust na telefonním čísle pro vaši zemi nebo e-mailem na adresu americanexpresscompliance@securetrust.com.
- **Zabezpečená linka pro faxy:** Ověřovací dokumentace může být zaslána faxem na: +1 (312) 276-4019. (+ značí mezinárodní předčísli IDD pro mezinárodní přímou volbu čísla, platí sazba pro mezinárodní hovory). Uvedte prosím vaše jméno, obchodní název, jméno vašeho kontaktu pro zabezpečení údajů, vaši adresu a telefonní číslo a, pouze v případě Obchodníků, 10místné číslo Obchodníka American Express.

Jestliže máte obecné dotazy o programu či výše uvedeném postupu, kontaktujte prosím společnost SecureTrust na + 800 9000 1140 nebo +1 (312) 267-3208 nebo e-mailem na adresu americanexpresscompliance@securetrust.com.

Náklady spojené s plněním požadavků a ověřováním nesete vy. Předložením Ověřovací dokumentace společnosti American Express vyjadřujete a zaručujete, že máte oprávnění ke zpřístupnění informací uvedených v těchto dokumentech a že Ověřovací dokumentaci společnosti American Express poskytujete bez porušení práv jakýchkoli dalších stran.

Trhy	Telefonní číslo na SecureTrust
Argentina	+ 800 9000 1140
Austrálie	+ 800 9000 1140
Bulharsko	+ 312 267 3208
Česká republika	+ 800 144 316
Chorvatsko	+ 312 267 3208
Dánsko	+ 800 9000 1140
Estonsko	+ 312 267 3208
Francie	+ 800 9000 1140
Hongkong	+ 800 9000 1140
IDC	+ 888 900 0114
Indie	+ 800 9000 1140
Irsko	+ 800 9000 1140
Island	+ 800 9000 1140
Itálie	+ 800 9000 1140
Japonsko	+ 312 267 3208
Kanada	1 866 659 9016
Kypr	+ 800 9000 1140
Litva	+ 312 267 3208
Lotyšsko	+ 312 267 3208
Maďarsko	+ 800 9000 1140
Malta	+ 312 267 3208

Trhy	Telefonní číslo na SecureTrust
Mexiko	+ 888 900 0114
Německo	+ 800 9000 1140
Nizozemsko	+ 312 267 3208
Norsko	+ 800 9000 1140
Nový Zéland	+ 800 9000 1140
Polsko	+ 800 9000 1140
Portugalsko	+ 312 267 3208
Rakousko	+ 800 9000 1140
Řecko	+ 312 267 3208
Rumunsko	+ 312 267 3208
Rusko	+ 312 267 3208
Singapur	+ 800 9000 1140
Slovensko	+ 312 267 3208
Slovinsko	+ 312 267 3208
Španělsko	+ 800 9000 1140
Spojené království	+ 800 9000 1140
Spojené státy	1 866 659 9016
Švédsko	+ 800 9000 1140
Tchaj-wan	+ 312 267 3208
Thajsko	+ 800 9000 1140

+ značí mezinárodní předčísli IDD pro mezinárodní přímou volbu čísla, platí sazba pro mezinárodní hovory

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.

Zašlete dokumentaci společnosti American Express do příslušného termínu. Společnost American Express vás samostatně upozorní na příslušné termíny pro každé roční a čtvrtletní období. Poplatky, které platí pro vaši zemi, jsou uvedeny v tabulce poplatků za neověření níže.

Popis	Obchodník na úrovni 1 nebo Poskytovatel služeb na úrovni 1	Obchodník na úrovni 2, Poskytovatel služeb na úrovni 2 nebo Obchodník v programu STEP	Obchodník na úrovni 3 nebo na úrovni 4
Bude účtován poplatek za neověření, jestliže Ověřovací dokumentace není obdržena do prvního termínu.	Poplatek za 1. měsíc pro Úroveň 1	Poplatek za 1. měsíc pro Úroveň 2	Měsíční poplatek
Bude účtován dodatečný poplatek za neověření, jestliže Ověřovací dokumentace není obdržena do 30 dnů od prvního termínu.	Poplatek za 2. měsíc pro Úroveň 1	Poplatek za 2. měsíc pro Úroveň 2	
Bude účtován dodatečný poplatek za neověření, jestliže Ověřovací dokumentace není obdržena do 60 dnů od prvního termínu.	Poplatek za 3. měsíc pro Úroveň 1	Poplatek za 3. měsíc pro Úroveň 3	

Jestliže společnost American Express neobdrží vaši povinnou Ověřovací dokumentaci do 60 dnů od prvního termínu, má společnost American Express právo předčasně ukončit Smlouvu v souladu s jejími podmínkami a zároveň vám účtovat výše uvedené kumulativní poplatky za neověření.

Tabulka poplatků za neověření

Trh	Úroveň	Typ	Měna	Poplatek za 1. měsíc	Poplatek za 2. měsíc	Poplatek za 3. měsíc
Austrálie	Úroveň 1	Obchodník nebo Poskytovatel služeb	AUD	35 000	49 000	63 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	AUD	7 000	14 000	21 000
	Úroveň 3 a Úroveň 4	Obchodník	AUD	Měsíční poplatek: 20		
Bulharsko	Úroveň 1	Obchodník nebo Poskytovatel služeb	BGN	28 000	40 000	51 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	BGN	5 500	11 000	16 500
	Úroveň 3 a Úroveň 4	Obchodník	BGN	Měsíční poplatek: 33		

Trh	Úroveň	Typ	Měna	Poplatek za 1. měsíc	Poplatek za 2. měsíc	Poplatek za 3. měsíc
Chorvatsko	Úroveň 1	Obchodník nebo Poskytovatel služeb	HRK	105 000	152 000	195 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	HRK	21 000	42 000	63 000
	Úroveň 3 a Úroveň 4	Obchodník	HRK	Měsíční poplatek: 130		
Kypr, Estonsko, Francie, Německo, Irsko, Španělsko, Lotyšsko, Litva, Portugalsko, Slovensko, Slovinsko	Úroveň 1	Obchodník nebo Poskytovatel služeb	EUR	19 000	26 000	34 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	EUR	4 000	7 500	11 000
	Úroveň 3 a Úroveň 4	Obchodník	EUR	Měsíční poplatek: 15		
Česká republika	Úroveň 1	Obchodník nebo Poskytovatel služeb	Kč	392 000	564 000	721 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	Kč	78 300	157 000	235 000
	Úroveň 3 a Úroveň 4	Obchodník	Kč	Měsíční poplatek: 440		
Dánsko	Úroveň 1	Obchodník nebo Poskytovatel služeb	DKK	110 000	156 000	200 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	DKK	22 000	42 000	65 000
	Úroveň 3 a Úroveň 4	Obchodník	DKK	Měsíční poplatek: 130		
Hongkong	Úroveň 1	Obchodník nebo Poskytovatel služeb	HKD	25 000	35 000	45 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	HKD	5 000	10 000	15 000
	Úroveň 3 a Úroveň 4	Obchodník	HKD	Měsíční poplatek: 150		

Trh	Úroveň	Typ	Měna	Poplatek za 1. měsíc	Poplatek za 2. měsíc	Poplatek za 3. měsíc
Maďarsko	Úroveň 1	Obchodník nebo Poskytovatel služeb	HUF	4 650 000	6 700 000	8 600 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	HUF	930 000	1 860 000	2 800 000
	Úroveň 3 a Úroveň 4	Obchodník	HUF	Měsíční poplatek: 5 500		
Island	Úroveň 1	Obchodník nebo Poskytovatel služeb	ISK	3 070 000	4 300 000	5 500 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	ISK	615 000	920 000	1 227 200
	Úroveň 3 a Úroveň 4	Obchodník	ISK	Měsíční poplatek: 2 400		
Nový Zéland	Úroveň 1	Obchodník nebo Poskytovatel služeb	NZD	35 000	49 000	63 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	NZD	7 000	14 000	21 000
	Úroveň 3 a Úroveň 4	Obchodník	NZD	Měsíční poplatek: 20		
Norsko	Úroveň 1	Obchodník nebo Poskytovatel služeb	NOK	135 000	195 000	249 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	NOK	27 000	54 000	81 000
	Úroveň 3 a Úroveň 4	Obchodník	NOK	Měsíční poplatek: 170		

Trh	Úroveň	Typ	Měna	Poplatek za 1. měsíc	Poplatek za 2. měsíc	Poplatek za 3. měsíc
Singapur	Úroveň 1	Obchodník nebo Poskytovatel služeb	SGD	38 000	53 000	68 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	SGD	7 500	15 000	22 500
	Úroveň 3 a Úroveň 4	Obchodník	SGD	Měsíční poplatek: 25		
Švédsko	Úroveň 1	Obchodník nebo Poskytovatel služeb	SEK	175 000	245 000	315 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	SEK	35 000	70 000	105 000
	Úroveň 3 a Úroveň 4	Obchodník	SEK	Měsíční poplatek: 135		
Spojené království	Úroveň 1	Obchodník nebo Poskytovatel služeb	GBP	12 500	18 000	23 000
	Úroveň 2	Obchodník nebo Poskytovatel služeb	GBP	2 500	5 000	7 500
	Úroveň 3 a Úroveň 4	Obchodník	GBP	Měsíční poplatek: 15		

Článek 5

Ochrana důvěrných informací

Společnost American Express přijme přiměřená opatření (a zajistí, aby přiměřená opatření přijali i její zmocněnci a subdodavatelé, včetně společnosti SecureTrust) 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:

- jsou společnosti American Express známy již před zpřístupněním;
- jsou nebo se stanou veřejně známými, aniž by společnost American Express porušila ustanovení tohoto odstavce;
- byly společnostmi American Express legálně získány od třetí strany bez povinnosti ochrany důvěrných informací;
- jsou nezávisle vyvinuty společnostmi American Express; nebo
- 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 6 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), AŽ 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 zneužití 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;
- 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.

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

Informace o držiteli karty znamená informace o Držiteli 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 jejich přidružených společností a vydanou vydavatelem, nebo číslo účtu karty.

Kredit znamená částku Platby, kterou Držitel 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 POS 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.

Období data incidentu znamená období, které začíná dnem incidentu, pokud je znám, nebo 365 dní před Dnem upozornění, pokud není znám skutečný den incidentu, a končí 30 dní po Dnu upozornění.

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.

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 zabezpečení údajů platebních karet při použití platebních aplikací (Payment Card Industry Payment Application Data Security Standard), která je k dispozici na adrese 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.

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

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 vylepšení zabezpečovací technologie neboli STEP (Security Technology Enhancement Program) znamená program společnosti American Express, ve kterém jsou Obchodníci motivováni k nasazování technologií zlepšujících zabezpečení dat. Aby Obchodníci mohli splnit kritéria pro program STEP, nesmí mít žádný Data incident za posledních 12 měsíců před předložením Výročního potvrzení STEP a musí provádět nejméně 75 % všech Transakcí využívajících Point-to-point šifrování nebo tzv. face to face Transakce pomocí Čipových zařízení EMV.

Shrnutí plnění požadavků nebo SOC (Summary of Compliance) znamená ověřovací dokument PCI používaný Franšízorem za účelem označení stavu souladu s požadavky PCI u příslušných Franšízantů.

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.

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

Systém Prodejněho 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.

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 (CSCCK, Klíče zabezpečení kódů karet)
- Klíče kódů PIN: Base Derivation Keys (BDK, Základní derivační klíče), PIN Encryption Key (PEK, Klíče šifrování kódů PIN) a ZPK

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: EMV, Point-to-Point šifrování a tokenizace.

Transakce znamená Platbu nebo Kredit realizovaný 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.

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.