AMERICAN EXPRESS

Datu drošības darbības politika (DSOP)

AMERICAN EXPRESS

DSOP izmaiņu kopsavilkums

Ikonas

Svarīgi atjauninājumi ir uzskaitīti Izmaiņu kopsavilkuma tabulā un norādīti arī *DSOP*, izmantojot izmaiņu joslu. Izmaiņu josla ir vertikāla līnija, parasti kreisajā piemalē, kas identificē pievienoto vai pārskatīto tekstu. Ar izmaiņu joslu, kā parādīts kreisajā piemalē, tiek norādītas tikai būtiskas izmaiņas *DSOP*, kas var ietekmēt Tirgotāja darbības procedūras.

Noņemtais teksts tiek iezīmēts ar atkritnes ikonu, kas novietota piemalē blakus jebkuram nozīmīgam teksta dzēsumam, iekļaujot sadaļas, tabulas, rindkopas, piezīmes un aizzīmju punktus. Lai izvairītos no pārpratumiem, noņemtajam tekstam šajā Izmaiņu kopsavilkumā ir atsauce, izmantojot iepriekšējās publikācijas sadaļu numerāciju.

Zilas līnijas, kas norobežo rindkopas, norāda reģiona specifisko informāciju.

Izmaiņu kopsavilkuma tabula

Svarīgi atjauninājumi ir uzskaitīti nākamajā tabulā un norādīti arī *DSOP*, izmantojot izmaiņu joslu.

Sadaļa/apakšsadaļa	Izmaiņu apraksts
Šajā relīzē nav izmaiņu.	

Sadaļa 1 Ievads DSOP un aizsardzības standarti

Kā līderim patērētāju aizsardzības jomā uzņēmumam American Express ir ilgtermiņa apņemšanās aizsargāt Kartes īpašnieka informāciju un Sensitīvos autentifikācijas datus, nodrošinot to drošu glabāšanu.

Apdraudēti dati negatīvi ietekmē patērētājus, Tirgotājus, Pakalpojumu sniedzējus un karšu izdevējus. Pat viens incidents var nodarīt nopietnu kaitējumu uzņēmuma reputācijai un mazināt tā spēju efektīvi veikt komercdarbību. Šo draudu novēršana, īstenojot drošības darbības politiku, var palīdzēt vairot klientu uzticību, palielināt rentabilitāti un uzlabot uzņēmuma reputāciju.

American Express zina, ka arī mūsu Tirgotāji un Pakalpojumu sniedzēji (kopā jūs) ir nobažījušies par to un pieprasa, lai **jūs**, pildot savus pienākumus, ievērotu datu drošības noteikumus savā līgumā par American Express® Kartes pieņemšanu (Tirgotāju gadījumā) vai apstrādāšanu (Pakalpojumu sniedzēju gadījumā) (katrs attiecīgi **Līgums**) un šo Datu drošības darbības politiku (DSOP), kuru mēs laiku pa laikam varam grozīt. Šīs prasības attiecas uz visām jūsu iekārtām, sistēmām un tīkliem (un to komponentiem), kur tiek glabātas, apstrādātas vai pārraidītas Šifrēšanas atslēgas, Kartes īpašnieka dati vai Sensitīvie autentifikācijas dati (vai to kombinācija).

Ar lielo sākuma burtu rakstītajiem terminiem, kuri šeit lietoti, bet nav definēti, ir šīs politikas beigās terminu sarakstā sniegtā nozīme.

Datu drošības darbības politika (DSOP) ir visaptverošu politikas prasību kopums, kas ir izstrādāts, lai aizsargātu Konta datus ikreiz, kad šādi dati tiek glabāti, apstrādāti vai pārsūtīti.

American Express pieprasa, lai visi Tirgotāji un Pakalpojumu sniedzēji ievērotu Maksājumu karšu nozares datu drošības standartu (PCI DSS). Darbības, kas šīs prasības ietvaros ir jāveic jums un jāliek veikt jūsu Aptvertajām personām:

- jāglabā Kartes īpašnieka dati vienīgi ar nolūku veicināt American Express Kartes darījumus saskaņā ar Līgumu un atbilstoši Līguma prasībām;
- jāievēro spēkā esošās PCI DSS un citas PCI drošības standartu padomes (PCI-SSC) prasības, kas ir attiecināmas uz jūsu Šifrēšanas atslēgu, Karšu īpašnieku datu vai Sensitīvo autentifikācijas datu apstrādi, glabāšanu vai pārsūtīšanu, ne vēlāk kā šīs piemērojamās prasības versijas īstenošanas spēkā stāšanās datumā;
- jānodrošina, ka tiek izmantoti PCI apstiprināti produkti, izvietojot vai aizstājot tehnoloģiju datu glabāšanai, apstrādei vai pārsūtīšanai.

Jums ir jāaizsargā visi American Express Maksājuma ieraksti un Kredīta ieraksti, kas tiek saglabāti saskaņā ar Līgumu atbilstoši šiem datu drošības noteikumiem; jums ir jāizmanto šie ieraksti vienīgi Līguma mērķiem un tie atbilstoši jāaizsargā. Jūs uzņematies finansiālu un cita veida atbildību pret American Express par to, lai nodrošinātu, ka jūsu Aptvertās personas ievēro šos datu drošības noteikumus (izņemot nolūku pierādīt, ka jūsu Aptvertās personas ievēro šo politiku saskaņā ar turpmāk esošo Sadaļa 2, „PCI DSS Atbilstības programma (Svarīga periodiska jūsu sistēmu validācija)“, ja vien šajā sadaļā nav noteikts citādi). Sīkāku informāciju par PCI standartiem un to prasību ievērošanu skatiet vietnē www.pcisecuritystandards.org.

Sadaļa 2 PCI DSS Atbilstības programma (Svarīga periodiska jūsu sistēmu validācija)

Jums ir jāveic turpmāk minētās darbības, lai saskaņā ar PCI DSS katru gadu un reizi 90 dienās pārbaudītu, kā aprakstīts turpmāk, to jūsu un jūsu Franšīzes ņēmēju iekārtu, sistēmu un/vai tīklu (un to komponentu) statusu, kuros tiek glabāti, apstrādāti vai pārraidīti Kartes īpašnieka dati vai Sensitīvie autentifikācijas dati.

Lai pabeigtu validāciju, jāveic četras darbības:

- Darbība 1: Dalība American Express Atbilstības programmā atbilstoši šai politikai.
- Darbība 2: Sava Tirgotāja/Pakalpojuma sniedzēja līmeņa un Validācijas dokumentācijas prasību izprašana.
- Darbība 3: American Express nosūtāmās Validācijas dokumentācijas aizpildīšana.
- Darbība 4: Validācijas dokumentācijas nosūtīšana American Express noteiktajā laikā.

Darbība 1: Dalība American Express Atbilstības programmā atbilstoši šai politikai

1. līmeņa Tirgotājiem, 2. līmeņa Tirgotājiem un visiem Pakalpojumu sniedzējiem, kā aprakstīts tālāk, ir jāpiedalās Programmā atbilstoši šai politikai. American Express pēc saviem ieskatiem var pieprasīt noteiktiem 3. līmeņa un 4. līmeņa Tirgotājiem piedalīties Programmā atbilstoši šai politikai.

Tirgotājam un Pakalpojumu sniedzējiem, kuriem jāpiedalās Programmā, ir jāreģistrējas American Express izvēlētā Programmas administratora nodrošinātajā Portālā norādītajos termiņos.

- Jums ir jāpieņem visi saprātīgie ar Portāla lietošanu saistītie noteikumi un nosacījumi.
- Portālā jums ir jānorāda un jāsniedz precīza informācija par vismaz vienu datu drošības kontaktpersonu. Nepieciešamajā informācijā ir iekļauts:
  - Pilns vārds
  - E-pasta adrese
  - Tālruņa numurs
  - Pasta adrese
- Kad informācija mainās, Portālā ir jānorāda atjaunināta vai jauna kontaktinformācija par nozīmēto datu drošības kontaktpersonu.
- Lai no Portāla domēna saņemtu servisa paziņojumus, jums ir jānodrošina savu sistēmu atjaunināšana.

Ja netiek iesniegta vai atjaunināta aktuālā datu drošības kontaktpersonas informācija vai netiek iespējoti e-pasta paziņojumi, tas neietekmē mūsu tiesības aprēķināt maksas.

Darbība 2: Sava Tirgotāja/Pakalpojuma sniedzēja līmeņa un Validācijas dokumentācijas prasību izprašana

Tirgotājiem ir noteikti četri Tirgotāju līmeņi, un Pakalpojumu Sniedzējiem - divi līmeņi, pamatojoties uz jūsu American Express Karšu Darījumu apjomu.

- Tirgotājiem tas ir to lestāžu iesniegtais apjoms, kas atbilst augstākajam American Express Tirgotāja konta līmenim.*
- Pakalpojumu sniedzējiem tā ir Pakalpojumu sniedzēja un Uzņēmumu pakalpojumu sniedzēja, kuram sniedzat pakalpojumus, apjomu summa.

Pircēju ierosināto maksājumu (BIP) darījumi netiek iekļauti American Express Karšu darījumu apjomā Tirgotāja līmeņa un validācijas prasību noteikšanas nolūkā. Jūs klasificēs vienā no Tirgotāju līmeņiem, kas norādīti Tabula A-1: Tirgotāju un Pakalpojumu sniedzēju līmeņi.

* Franšīzes devēju gadījumā tas ietver apjomu no viņu Franšīzes ņēmēju lestādēm. Franšīzes devējiem, kuri pieprasa, lai viņu Franšīzes ņēmēji izmantotu konkrētu Pārdošanas punkta (POS) sistēmu vai Pakalpojumu sniedzēju, jāiesniedz arī validācijas dokumentācija par attiecīgajiem Franšīzes ņēmējiem.

Tabula A-1: Tirgotāju un Pakalpojumu sniedzēju līmeņi

Tirdzniecības pakalpojumu sniedzēja līmenis	American Express Darījumi gadā
1. līmeņa Tirgotājs	Vismaz 2,5 miljoni American Express Karšu darījumu gadā vai jebkurš Tirgotājs, kuru American Express citādi pieskaita 1. līmenim.
2. līmeņa Tirgotājs	No 50 000 līdz mazāk nekā 2,5 miljoniem American Express Karšu darījumu gadā.
3. līmeņa Tirgotājs	No 10 000 līdz mazāk nekā 50 000 American Express Karšu darījumu gadā.
4. līmeņa Tirgotājs	Mazāk nekā 10 000 American Express Karšu darījumu gadā.
Pakalpojumu sniedzēja līmenis	**American Express Darījumi gadā**
1. līmeņa Pakalpojumu sniedzējs	2,5 miljoni vai vairāk American Express Karšu darījumu gadā; vai jebkurš Pakalpojumu sniedzējs, kuru American Express citādi uzskata par 1. līmeņa Pakalpojumu sniedzēju.
2. līmeņa Pakalpojumu sniedzējs	Mazāk nekā 2,5 miljoni American Express Karšu darījumu gadā; vai jebkurš Pakalpojumu sniedzējs, kuru American Express citādi neuzskata par 1. līmeņa Pakalpojumu sniedzēju.

Tirgotāju Validācijas dokumentācijas prasības

Tirgotājiem (nevis Pakalpojumu sniedzējiem) ir četras iespējamās Tirgotāja līmeņa klasifikācijas. Pēc Tirgotāja līmeņa noteikšanas atbilstoši Tabula A-1: Tirgotāju un Pakalpojumu sniedzēju līmeņi (iepriekš) skatiet Tabula A-2: Tirgotāju Validācijas dokumentācija, lai noteiktu validācijas dokumentācijas prasības.

Tabula A-2: Tirgotāju Validācijas dokumentācija

Tirgotāja līmenis/ American Express Darījumi gadā	Ziņojums par atbilstību Atbilstības apstiprināšana (ROC AOC)	Pašnovērtējuma anketa Atbilstības apstiprināšana (SAQ AOC) UN Ikceturkšņa ārējās tīkla ievainojamības skenēšana (skenēšana)	Drošības tehnoloģiju uzlabošanas programmas (STEP) atestācija Tirgotājiem, kas kvalificējas
1. līmenis/ 2,5 miljoni vai vairāk	Obligāti	Nav attiecināms	Izvēles, ar American Express apstiprinājumu (aizstāj ROC)
2. līmenis/ no 50 000 līdz mazāk nekā 2,5 miljoniem	Izvēles	SAQ AOC obligāts (ja netiek iesniegts ROC AOC); skenēšana obligāta ar noteiktiem SAQ veidiem	Izvēles, ar American Express apstiprinājumu* (aizstāj SAQ un tīkla skenēšanu vai ROC)
3. līmenis**/ no 10 000 līdz mazāk nekā 50 000	Izvēles	SAQ AOC izvēles (obligāts, ja to pieprasa American Express); skenēšana obligāta ar noteiktiem SAQ veidiem	Izvēles, ar American Express apstiprinājumu* (aizstāj SAQ un tīkla skenēšanu vai ROC)
4. līmenis**/ mazāk nekā 10 000	Izvēles	SAQ AOC izvēles (obligāts, ja to pieprasa American Express); skenēšana obligāta ar noteiktiem SAQ veidiem	Izvēles, ar American Express apstiprinājumu* (aizstāj SAQ un tīkla skenēšanu vai ROC)

* **Piezīme:** American Express PCI komanda izskatīs pieprasījumu un piemērotību, kā arī apstiprinās, vai jūs kvalificējaties STEP programmai. Lūdzu, sazinieties ar savu klientu pārvaldnieku un/vai AXPPCIComplianceProgram@aexp.com, lai pārbaudītu atbilstību.

**Pārpratumu novēršanai ņemiet vērā, ka 3. līmeņa un 4. līmeņa Tirgotājiem nav jāiesniedz Validācijas dokumentācija, ja vien American Express to nenosaka pēc saviem ieskatiem, taču šiem Tirgotājiem ir jāatbilst, un tie ir atbildīgi par visu šīs Datu drošības darbības politikas noteikumu ievērošanu.

American Express patur tiesības pārbaudīt jūsu PCI Validācijas dokumentācijas pilnīgumu, precizitāti un atbilstību. Šajā nolūkā American Express var lūgt iesniegt izvērtēšanai papildu apliecinošos dokumentus. Turklāt American Express ir tiesības lūgt jūs piesaistīt PCI drošības standartu padomes apstiprinātu Kvalificētu drošības novērtētāju (QSA) vai PCI ekspertu (PFI).

Pakalpojumu sniedzēju Validācijas dokumentācijas prasības

Pakalpojumu sniedzējiem (nevis Tirgotājiem) ir noteiktas divas iespējamās līmeņa klasifikācijas. Pēc Pakalpojumu sniedzēja līmeņa noteikšanas atbilstoši Tabula A-1: Tirgotāju un Pakalpojumu sniedzēju līmeņi (iepriekš) skatiet Tabula A-3: Pakalpojumu sniedzēju Validācijas dokumentācija, lai noteiktu validācijas dokumentācijas prasības.

Pakalpojumu Sniedzēji nav tiesīgi saņemt STEP.

Tabula A-3: Pakalpojumu sniedzēju Validācijas dokumentācija

Līmenis	Validācijas dokumentācija	Prasība
1	Ikgadējais Ziņojums par atbilstību Atbilstības apstiprināšana (ROC AOC)	Obligāti
2	Ikgadējā SAQ D (Pakalpojumu sniedzējs) un Ikceturkšņa tīkla skenēšana vai Ikgadējais Ziņojums par atbilstību Atbilstības apstiprināšana (ROC AOC), ja izvēlas to	Obligāti

Ieteicams, lai Pakalpojumu sniedzēji nodrošinātu atbilstību ar PCI noteikto papildu validāciju noteiktiem uzņēmumiem.

Drošības tehnoloģiju uzlabošanas programma (STEP)

Tirgotāji, kas atbilst PCI DSS, pēc American Express ieskatiem var kvalificēties drošības tehnoloģijas uzlabošanas programmai (STEP), ja viņi savās Karšu apstrādes vidēs ievieš noteiktas papildu drošības tehnoloģijas. STEP ieviešama tikai tādā gadījumā, ja Tirgotājs iepriekšējos 12 mēnešos nav piedzīvojis Datu incidentu un 75 % no visiem Tirgotāja Karšu Darījumiem tiek veikti, izmantojot šādu uzlabotās drošības iespēju kombināciju:

- **EMV, EMV bezkontakta vai digitālais maks** – aktīvā Mikroshēmā iespējotā ierīcē, kurai ir derīgs un spēkā esošs EMVCo (www.emvco.com) apstiprinājums/sertifikācija un kas spēj apstrādāt AEIPS prasībām atbilstošus Mikroshēmas karšu darījumus. (ASV Tirgotājiem jāiekļauj bezkontakta)
- **Divpunktu šifrēšanu (P2PE)** – kas paziņota Tirgotāja starpniekiestādei, izmantojot PCI SSC apstiprinātu vai QSA apstiprinātu Divpunktu šifrēšanas sistēmu
- **Tokenizēts** – ieviestajam tokenizācijas risinājumam:
  - jāatbilst EMVCo specifikācijām,
  - jāsargā, jāapstrādā, jāglabā, jāpārsūta un pilnīgi jāpārvalda PCI atbilstošam trešās puses pakalpojumu sniedzējam, un
  - nedrīkst būt iespēja dekompilēt Tokenu, lai Tirgotājam atklātu atmaskotus Primārā konta numurus (PAN).

Tirgotājiem, kuri ir tiesīgi saņemt Drošības tehnoloģiju uzlabošanas programmu, ir samazinātas PCI Validācijas dokumentācijas prasības, kā aprakstīts turpmāk Darbība 3: „American Express nosūtāmās Validācijas dokumentācijas aizpildīšana“ zemāk.

Darbība 3: American Express nosūtāmās Validācijas dokumentācijas aizpildīšana

Turpmāk minētie dokumenti ir nepieciešami dažādiem Tirgotāju un Pakalpojumu sniedzēju līmeņiem, kas uzskaitīti Tabula A-2: Tirgotāju Validācijas dokumentācija un Tabula A-3: Pakalpojumu sniedzēju Validācijas dokumentācija iepriekš.

Jums ir jāiesniedz Atbilstības apstiprināšana (AOC) atbilstoši piemērojamam novērtējuma tipam. AOC ir jūsu atbilstības statusa deklarācija, un tā ir jāparaksta un jādatē atbilstoša līmeņa vadībai jūsu organizācijā.

Papildus AOC American Express var pieprasīt iesniegt pilna novērtējuma kopiju un, pēc mūsu ieskatiem, papildu apliecinošos dokumentus, kas apliecina atbilstību PCI DSS prasībām. Šī Validācijas dokumentācija tiek aizpildīta uz jūsu rēķina.

Ziņojums par atbilstību Atbilstības apstiprināšana (ROC AOC) – (Ikgadējā prasība) - Ziņojumā par atbilstību ir aprakstīti rezultāti jūsu iekārtu, sistēmu un tīklu (un to komponentu), kuros tiek glabāti, apstrādāti vai pārraidīti Kartes turētāja dati vai Sensitīvie autentifikācijas dati (vai abi), detalizētai pārbaudei uz vietas. Ir divas versijas: viena paredzēta Tirgotājiem un otra - Pakalpojumu sniedzējiem. Ziņojums par atbilstību jāsagatavo:

- QSA vai
- Iekšējās drošības novērtētājam (ISA) un jāapstiprina jūsu izpilddirektoram, finanšu direktoram, galvenajam informācijas drošības speciālistam vai vadītājam

ROC AOC ir jāparaksta un jādatē QSA vai ISA un pilnvarota līmeņa vadībai jūsu organizācijā un jāiesniedz American Express vismaz vienreiz gadā.

Pašnovērtējuma anketa Atbilstības apstiprināšana (SAQ AOC) – (Ikgadējā prasība) – Pašnovērtējuma anketas ļauj veikt pašpārbaudi jūsu iekārtām, sistēmām un tīkliem (un to komponentēm), kur tiek glabāti, apstrādāti vai pārsūtīti Kartes turētāja dati vai Sensitīvie autentifikācijas dati (vai abi). Ir vairākas SAQ versijas. Jūs izvēlēsieties vienu vai vairākas versijas atkarībā no jūsu Kartes turētāja datu vides.

SAQ jāaizpilda jūsu Uzņēmuma personālam, kas ir kvalificēts atbildēt uz tās jautājumiem precīzi un pamatīgi, vai arī varat iesaistīt QSA. SAQ AOC jāparaksta un jādatē pilnvarota līmeņa vadībai jūsu organizācijā un jāiesniedz American Express vismaz reizi gadā.

Apstiprinātais skenēšanas pakalpojumu sniedzēja ārējās tīkla ievainojamības skenēšanas kopsavilkums (ASV skenēšana) - (90 dienu prasība) – Ārējās ievainojamības skenēšana ir attālināts tests, kas palīdz identificēt jūsu Kartes turētāja datu vides internetā pieejamo komponentu (piemēram, tīmekļa vietņu, lietotņu, tīmekļa serveru, pasta serveru, publiski pieejamo domēnu vai resursdatoru) potenciālās vājās vietas, ievainojamības un nepareizas konfigurācijas.

ASV skenēšana jāveic Apstiprinātam skenēšanas pakalpojumu sniedzējam (ASV).

Ja to pieprasa SAQ, ASV skenēšanas ziņojums Skenēšanas atbilstības apstiprinājums (AOSC) vai ziņojuma kopsavilkums, norādot skenēto mērķus skaitu, apliecinājumu, ka rezultāti atbilst PCI DSS skenēšanas procedūrām, un ASV veiktās skenēšanas statusu, jāiesniedz American Express vismaz reizi 90 dienās.

Ja iesniedzat ROC AOC vai STEP, jums nav pienākuma iesniegt AOSC vai ASV skenēšanas ziņojuma kopsavilkumu, ja tas netiek īpaši pieprasīts. Lai izvairītos no šaubām, skenēšanas ir obligātas, ja to pieprasa atbilstošā SAQ.

STEP atestācijas Validācijas dokumentācija (STEP) – (ikgadējā prasība) – STEP ir pieejama tikai Tirgotājiem, kuri atbilst kritērijiem, kas norādīti Darbība 2: „Sava Tirgotāja/Pakalpojuma sniedzēja līmeņa un Validācijas dokumentācijas prasību izprašana“ iepriekš. Ja jūsu uzņēmums kvalificējas, jums katru gadu ir jāaizpilda un jāiesniedz American Express STEP Atestācijas veidlapa. Ikgadējās STEP Atestācijas veidlapa lejupielādei ir pieejama Portālā. Varat arī sazināties ar savu klientu menedžeri vai rakstīt American Express uz AXPPCIComplianceProgram@aexp.com.

Neatbilstība PCI DSS – (ikgadējā, 90 dienu un/vai Ad Hoc prasība) – ja neatbilstat PCI DSS, jums ir jāiesniedz PCI Prioritārās pieejas rīka (PAT) kopsavilkums (pieejams lejupielādei no PCI drošības standartu padomes tīmekļa vietnes).

Katrā no iepriekš minētajiem dokumentiem PAT kopsavilkumā ir jānosaka novēršanas termiņš, kas nepārsniedz divpadsmit (12) mēnešus pēc dokumenta pabeigšanas datuma, lai sasniegtu atbilstību. Jums ir regulāri jāinformē American Express par sava Neatbilstības statusa problēmas novēršanas progresu (1. līmeņa, 2. līmeņa, 3. līmeņa un 4. līmeņa Tirgotāji; visi Pakalpojumu sniedzēji). Novēršanas darbības, kas nepieciešamas atbilstības ar PCI DSS sasniegšanai, ir jāveic uz jūsu rēķina.

American Express nepiemēro neatbilstības maksu pirms novēršanas termiņa. Saskaņā ar Tabula A-4: Neatbilstības maksa jūs joprojām esat atbildīgs American Express par visām atlīdzības saistībām saistībā ar Datu incidentu, un uz jums attiecas visi pārējie šīs politikas noteikumi.

American Express pēc saviem ieskatiem patur tiesības noteikt neatbilstības maksu, ja:

- PCI Prioritārās pieejas veidne nav iesniegta saskaņā ar šajā sadaļā noteiktajām prasībām;

- PCI Prioritārās pieejas veidnē nav izpildītas neatbilstības statusam norādītās novēršanas darbības;
- nav izpildīta kāda no PCI Prioritārās pieejas veidnes prasībām par neatbilstības statusu; vai
- obligātā atbilstības dokumentācija nav iesniegta American Express noteiktajā termiņā vai pēc pieprasījuma.

Tirgotājiem/pakalpojumu sniedzējiem, kas neatbilst Darbība 2: Sava Tirgotāja/Pakalpojuma sniedzēja līmeņa un Validācijas dokumentācijas prasību izprašana prasībām, var tikt piemērota maksa, kā norādīts Darbība 4: Validācijas dokumentācijas nosūtīšana American Express.

Lai izvairītos no pārpratumiem, Tirgotāji, kas neatbilst PCI DSS, nekvalificējas STEP.

Darbība 4: Validācijas dokumentācijas nosūtīšana American Express

Visiem Tirgotājiem un Pakalpojumu sniedzējiem, kuriem jāpiedalās Programmā, ir jāiesniedz Validācijas dokumentācija, kas atzīmēta kā "obligāta" Darbība 2: „Sava Tirgotāja/Pakalpojuma sniedzēja līmeņa un Validācijas dokumentācijas prasību izprašana“, American Express piemērojamajos termiņos.

Jums ir jāiesniedz sava Validācijas dokumentācija American Express, izmantojot Portālu, ko nodrošina American Express izvēlētais Programmas administrators. Iesniedzot Validācijas dokumentāciju, jāapliecina un jāgarantē American Express, ka tā ir patiesa (cik iespējams):

- Jūsu novērtējums bija pilnīgs un pamatīgs;
- PCI DSS statuss pabeigšanas brīdī ir norādīts precīzi neatkarīgi no tā, vai tiek iesniegts Atbilstības apstiprinājums (AOC) vai PCI Prioritārās pieejas rīka (PAT) kopsavilkums par neatbilstību;
- Jums ir tiesības atklāt tajā iekļauto informāciju un iesniegt Validācijas dokumentāciju American Express, nepārkāpjot citas puses tiesības.

Neatbilstības maksa un Līguma izbeigšana

American Express ir tiesības iekasēt no jums neatbilstības maksas un izbeigt Līgumu, ja jūs neizpildāt šīs prasības vai neiesniedzat obligāto Validācijas dokumentāciju American Express līdz noteiktajam termiņam. American Express mēģinās paziņot datu drošības kontaktpersonai katram gada un ceturkšņa pārskata periodam piemērojamo termiņu.

Tabula A-4: Neatbilstības maksa

Apraksts*	1. līmeņa Tirgotājs vai 1. līmeņa Pakalpojumu sniedzējs	2. līmeņa Tirgotājs vai 2. līmeņa Pakalpojumu sniedzējs	3. līmeņa vai 4. līmeņa Tirgotājs
Neatbilstības maksu aprēķina, ja Validācijas dokumentācija nav saņemta līdz pirmajam termiņam.	$25 000 USD	$5000 USD	$50 USD
Papildu neatbilstības maksu aprēķina, ja Validācijas dokumentācija nav saņemta līdz otrajam termiņam.	$35 000 USD	$10 000 USD	$100 USD
Papildu neatbilstības maksu aprēķina, ja Validācijas dokumentācija nav saņemta līdz trešajam termiņam. **PIEZĪME:** neatbilstības maksas tiek piemērotas, līdz tiek iesniegta Validācijas dokumentācija.	$45 000 USD	$15 000 USD	$250 USD

* Neatbilstības maksas tiks noteiktas Vietējās valūtas ekvivalentā.

* Nav attiecināms uz Argentīnu.

Ja jūsu PCI DSS atbilstības dokumentācijas pienākumi nav izpildīti, American Express ir tiesības piemērot neatbilstības maksas kumulatīvi, ieturēt maksājumus un/vai izbeigt Līgumu.

Sadaļa 3 Datu incidentu pārvaldības pienākumi

Jums nekavējoties un nekādā gadījumā ne vēlāk kā septiņdesmit divas (72) stundas pēc Datu incidenta atklāšanas ir jāinformē par to American Express.

Lai informētu American Express, lūdzu, sazinieties ar American Express Uzņēmumu Incidentu Reaģēšanas programmu [Enterprise Incident Response Programme] (*EIRP*) bez maksas 1 888 732 3750 vai 1 602 537 3021, vai e-pastā uz adresi EIRP@aexp.com. Jums ir jānorāda sava kontaktpersona saistībā ar šādu Datu incidentu. Papildus tam:

- jums ir rūpīgi jāizpēta katrs Datu incidents un nekavējoties jāiesniedz American Express visi apdraudēto Karšu numuri. American Express patur tiesības veikt iekšēju analīzi, lai identificētu ar Datu incidentu saistītos datus.

Par Datu incidentiem, kas ir saistīti ar mazāk nekā 10 000 unikālu Karšu numuru, izmeklēšanas kopsavilkums American Express ir jāiesniedz desmit (10) darbdienu laikā pēc tā pabeigšanas.

- Izmeklēšanas kopsavilkumos iekļaujamā informācija: incidentu kopsavilkums, ietekmētās vides apraksts, notikumu laika grafiks, galvenie datumi, ietekmes un datu izpaušanas informācija, ierobežošanas un novēršanas darbības, kā arī apliecinājums, ka nav pazīmju par citu American Express datu apdraudējumu.

Datu incidentu, kas skar 10 000 vai vairāk unikālo Karšu numuru, gadījumā jums ir jāpiesaista PCI PFI izmeklēšanas veikšanai piecu (5) dienu laikā pēc Datu incidenta atklāšanas.

- Nerediģēts izmeklēšanas ziņojums jāiesniedz American Express desmit (10) darbdienu laikā pēc izmeklēšanas pabeigšanas.
- Izmeklēšanas ziņojumi ir jāaizpilda, izmantojot pašlaik no PCI pieejamo Izmeklēšanas incidenta galīgā ziņojuma veidni. Šādā ziņojumā ir jāietver izmeklēšanas pārskati, atbilstības ziņojumi un visa pārējā informācija, kas ir saistīta ar Datu incidentu; jāidentificē Datu incidenta iemesls; jāapstiprina, vai Datu aizsardzības pārkāpuma brīdī ievērojāt PCI DSS; un jāapliecina sava spēja novērst turpmākos Datu incidentus, (i) iesniedzot plānu visu PCI DSS trūkumu novēršanai un (ii) piedaloties American Express atbilstības programmā (kā minēts tālāk). Pēc American Express pieprasījuma jums ir jāiesniedz Kvalificēta drošības vērtētāja (QSA) apliecinājums, ka nepilnības ir novērstas.

Neatkarīgi no šīs "Sadaļa 3. „Datu incidentu pārvaldības pienākumi“:

- American Express var pēc saviem ieskatiem pieprasīt jums iesaistīt PFI, lai veiktu tādu Datu incidentu izmeklēšanu, kuros ir iesaistīti mazāk nekā 10 000 unikālo Karšu numuru vai 12 mēnešu laikā ir notikuši vairāki incidenti. Visām šādām izmeklēšanām ir jāatbilst prasībām, kas noteiktas iepriekš šajā Sadaļa 3. „Datu incidentu pārvaldības pienākumi“, un tās ir jāveic American Express pieprasītajā termiņā.
- American Express var pēc saviem ieskatiem atsevišķi iesaistīt PFI, lai tas veiktu jebkura Datu incidenta izmeklēšanu, un var prasīt jums segt šādas izmeklēšanas izmaksas.

Jums ir jānovērtē Datu incidents saskaņā ar piemērojamiem globāliem datu aizsardzības pārkāpuma ziņošanas tiesību aktiem un, ja tas tiek uzskatīts par nepieciešamu, jāinformē attiecīgie regulatori un ietekmētie Karšu lietotāji saskaņā ar šādiem datu pārkāpumu ziņošanas tiesību aktiem. Ja esat noteicis, ka jūsu Pakalpojumu sniedzēja vai citas personas pienākums ir ziņot par Datu incidentu, jums ir šāds Pakalpojumu sniedzējs vai juridiskā persona jāinformē par tās pienākumu izvērtēt savus ziņošanas pienākumus saskaņā ar piemērojamiem datu pārkāpumu ziņošanas tiesību aktiem. Jūs piekrītat iegūt American Express rakstisku apstiprinājumu, pirms atsaucat vai nosaucat American Express jebkādā saziņā ar Kartes lietotājiem par Datu incidentu. Jūs piekrītat sadarboties ar American Express, lai sniegtu detalizētu informāciju un novērstu visas problēmas, kas izriet no Datu incidenta, tostarp sniedzot (un iegūstot jebkādas sniegšanai nepieciešamās atrunas) American Express visu attiecīgo informāciju, lai apstiprinātu savu spēju novērst turpmākus Datu incidentus Līgumam atbilstošā veidā.

Neraugoties uz Līgumā iekļautajiem citiem pretējiem konfidencialitātes ievērošanas pienākumiem, American Express ir tiesības atklāt informāciju par Datu incidentu American Express Karšu lietotājiem, izdevējiem, citiem American Express tīkla dalībniekiem un vispārējai sabiedrībai saskaņā ar Amerikas tiesību aktu prasībām; tiesas, administratīvu vai regulēšanas rīkojumu, dekrētu, pavēsti, pieprasījumu vai citu procesu; lai mazinātu krāpšanas vai cita kaitējuma risku; vai citādi tādā mērā, kas ir piemērots, lai nodrošinātu American Express tīkla darbību.

Ko darīt, ja ir noticis Datu incidents?

Ja jūsu uzņēmumā ir noticis Datu incidents, lūdzu, veiciet šādas darbības.

1. darbība:
Aizpildiet Tirgotāja Datu incidenta sākotnējās ziņošanas veidlapu un nosūtiet to e-pastā uz EIRP@aexp.com 72 stundu laikā kopš Datu incidenta atklāšanas.

2. darbība:
Veiciet rūpīgu izpēti; lai to izdarītu, varētu būt nepieciešams nolīgt Maksājumu karšu nozares (PCI) ekspertu.

3. darbība:
Nekavējoties nosūtiet mums visus apdraudētos American Express® Karšu numurus.

4. darbība:
Sadarbojieties ar mums, lai palīdzētu atrisināt jebkuras ar Datu incidentu saistītas problēmas.

Skatiet Sadaļa 3, „Datu incidentu pārvaldības pienākumi“ sīkāku informāciju par Datu incidentu pārvaldības pienākumiem.

Ir citi jautājumi?

ASV: (888) 732-3750 (bezmaksas)

Starptautiskais: +1 (602) 537-3021

EIRP@aexp.com

Sadaļa 4 Zaudējumu atlīdzības saistības Datu incidenta gadījumā

Jūsu Līgumā paredzētās saistības atlīdzināt uzņēmumam American Express zaudējumus par Datu Incidentiem tiek noteiktas, neatsakoties no jebkādām citām American Express tiesībām un tiesiskās aizsardzības līdzekļiem, saskaņā ar šo Sadaļa 4, „Zaudējumu atlīdzības saistības Datu incidenta gadījumā“. Papildus pienākumam atlīdzināt zaudējumus (ja tādi ir) jums var būt jāmaksā Datu incidenta neatbilstības maksa, kas aprakstīta turpmāk tekstā šajā Sadaļa 4, „Zaudējumu atlīdzības saistības Datu incidenta gadījumā“.

Jums ir jāmaksā kompensācija American Express saskaņā ar likmi $5 USD par vienu konta numuru Datu incidentos, kuros ir iesaistīti:

- 10 000 vai vairāk American Express Karšu numuri ar vienu no šeit norādītajiem:
  - Sensitīviem autentifikācijas datiem vai
  - Derīguma termiņu

Taču American Express nepieprasīs no jums kompensāciju par Datu incidentu, kurā iesaistīts:

- mazāk nekā 10 000 American Express Karšu numuru vai
- vairāk nekā 10 000 American Express Karšu numuru, ja jūs izpildāt šādus nosacījumus:
  - jūs ziņojāt American Express par Datu incidentu saskaņā ar Sadaļa 3, „Datu incidentu pārvaldības pienākumi“,
  - Datu incidenta brīdī jūs ievērojāt PCI DSS (kas konstatēts Datu incidenta PFI izmeklēšanā), un
  - Datu incidentu neizraisīja jūsu vai jūsu Aptverto personu nepareiza rīcība.

Neraugoties uz šīs Sadaļa 4, „Zaudējumu atlīdzības saistības Datu incidenta gadījumā“ iepriekšējiem punktiem, par katru Datu incidentu neatkarīgi no American Express Karšu skaita jūs maksājat American Express Datu incidenta neatbilstības maksu, kas nepārsniedz $100 000 USD par Datu incidentu (ko pēc saviem ieskatiem nosaka American Express), ja neizpildāt kādu no saviem pienākumiem, kas noteikti Sadaļa 3, „Datu incidentu

pārvaldības pienākumi". Lai izvairītos no šaubām, kopējā Datu incidenta neatbilstības maksa, kas aprēķināta par jebkuru atsevišķu Datu incidentu, nedrīkst pārsniegt $100 000 USD.

American Express izslēgs no saviem aprēķiniem jebkuru American Express Kartes konta numuru, kas bija iesaistīts iepriekšējā Datu incidenta kompensācijas prasībā, kas tikusi iesniegta divpadsmit (12) mēnešu laikā pirms Paziņošanas datuma. Visi saskaņā ar šo metodiku veiktie American Express aprēķini ir galīgi.

American Express var izsniegt jums rēķinu par jūsu kompensācijas saistību ar Datu incidentiem pilno summu vai atskaitīt šo summu no American Express maksājumiem jums (vai attiecīgi debetēt jūsu bankas Kontu) saskaņā ar Līgumu.

Jūsu saistības atlīdzināt zaudējumus par Datu incidentiem saskaņā ar šo nav uzskatāmas par nejaušiem, netiešiem, spekulatīviem, izrietošiem, īpašiem, soda vai parauga zaudējumu atlīdzības gadījumiem saskaņā ar Līgumu, ja šādas saistības neietver kaitējumus, kas saistīti ar peļņas vai ienākumu zaudējumu, nemateriālās vērtības zaudējumu vai komercdarbības iespēju zaudējumu.

American Express pēc saviem ieskatiem ir tiesības samazināt zaudējumu atlīdzību Tirgotājiem tikai par Datu incidentiem, kas atbilst šādiem kritērijiem:

- pirms Datu incidenta un visa Datu incidenta gadījumu loga laikā tika izmantotas attiecināmās Risku mazināšanas tehnoloģijas;
- ir pabeigta rūpīga izmeklēšana saskaņā ar PFI programmu (ja nav citas iepriekšējas rakstveida vienošanās);
- izmeklēšanas ziņojumā ir skaidri norādīts, ka Risku mazināšanas tehnoloģijas tika izmantotas, lai apstrādātu, glabātu un/vai sūtītu datus Datu incidenta laikā; un
- jūs neglabājāt (tostarp visā Datu incidenta gadījumu loga laikā) Sensitīvus autentifikācijas datus vai jebkurus Kartes īpašnieka datus, kas nav padarīti neizlasāmi.

Ja ir piemērojama zaudējumu atlīdzināšanas pienākuma apmēra samazināšana, tad jūsu zaudējumu atlīdzināšanas pienākuma apmērs (atskaitot jebkādas maksājamās neatbilstības maksas) tiek samazināts atbilstoši turpmāk norādītajam:

Tabula A-5: Zaudējumu atlīdzības saistību samazināšanas kritēriji

Atlīdzības saistību samazināšana	Nepieciešamie kritēriji
Standarta samazinājums: 50 %	>75 % no kopējo Darījumu skaita apstrādāti ar Mikroshēmas ierīcēm[1] VAI
	Riska mazināšanas tehnoloģija tiek izmantota >75 % Tirgotāja atrašanās vietu[2]
Paaugstināts samazinājums: no 75 % uz 100 %	>75 % no kopējo Darījumu skaita apstrādāti ar Mikroshēmas ierīcēm,[1] UN cita Riska mazināšanas tehnoloģija izmantota >75 % Tirgotāja atrašanās vietu[2]

[1] Noteikts American Express iekšējā analīzē

[2] Noteikts PFI izmeklēšanā

- Palielinātais samazinājums (no 75 % uz 100 %) tiek noteikts, ņemot vērā mazāko apmēru no Darījumiem, kuros tiek izmantotas Mikroshēmas ierīces, UN Tirgotāju vietas, kurās tiek izmantotas cita Risku mazināšanas tehnoloģija. Piemēri Tabula A-6: Zaudējumu atlīdzības saistību samazināšana ilustrē atlīdzības samazinājuma aprēķinu.
- Lai kvalificētos Risku mazināšanas tehnoloģijas izmantošanai, jums ir jādemonstrē efektīva tehnoloģijas izmantošana atbilstoši tās izstrādes un paredzētajam mērķim.
- Tirdzniecības vietu procentuālais īpatsvars, kas izmanto Risku mazināšanas tehnoloģiju, tiek noteikts PFI izmeklēšanā.

- Zaudējumu atlīdzināšanas pienākuma apmēra samazinājums neattiecas uz jebkuru neatbilstības maksu, kas maksājama saistībā ar Datu incidentu.

Tabula A-6: Zaudējumu atlīdzības saistību samazināšana

Piem	Izmantotās Riska mazināšanas tehnoloģijas	Piemērots	Samazinājums
1	• 80 % Darījumu ar Mikroshēmas ierīcēm • 0 % atrašanās vietu izmantota cita Riska mazināšanas tehnoloģija	Nē	50 %: Standarta samazinājums (mazāk kā 75 % Riska mazināšanas tehnoloģiju lietojums nekvalificējas Paaugstinātam samazinājumam)[1]
2	• 80 % Darījumu ar Mikroshēmas ierīcēm • 77 % atrašanās vietu izmantota cita Riska mazināšanas tehnoloģija	Jā	77 %: Paaugstināts samazinājums (pamatojoties uz 77 % Riska mazināšanas tehnoloģijas izmantošanu)
3	• 93 % Darījumu ar Mikroshēmas ierīcēm • 100 % atrašanās vietu izmantota cita Riska mazināšanas tehnoloģija	Jā	93 %: Paaugstināts samazinājums (pamatojoties uz 93 % Darījumu ar Mikroshēmas ierīcēm)
4	• 40 % Darījumu ar Mikroshēmas ierīcēm • 90 % atrašanās vietu izmantota cita Riska mazināšanas tehnoloģija	Nē	50 %: Standarta samazinājums (mazāk nekā 75 % Darījumu ar Mikroshēmas ierīcēm nekvalificējas Paaugstinātam samazinājumam)

[1] Datu incidents, kurā iesaistīti 10 000 American Express Karšu kontu, piemērojot $5,00 USD par katru konta numuru (10 000 x $5 USD = $50 000 USD), var kvalificēties 50 % samazinājumam (zaudējumu atlīdzināšanas pienākuma apmērs tiek samazināts no $50 000 USD uz $25 000 USD), atskaitot jebkādu neatbilstības maksu.

Sadaļa 5 Mērķtiecīga analīzes programma (TAP)

Kartes īpašnieka datu apdraudējumus var izraisīt datu drošības nepilnības jūsu Kartes īpašnieku datu vidē (CDE).

Kartes īpašnieka datu apdraudējuma piemēri ietver, bet nav aprobežoti ar turpmāk minēto:

- **Vienota pirkuma vieta (CPP):** American Express Karšu lietotāji ziņo par krāpnieciskiem Darījumiem savos Karšu kontos, un tiek identificēts un noteikts, ka tie radušies, veicot pirkumus jūsu lestādēs.
- **Atrasti Kartes dati:** American Express Kartes un Kartes īpašnieka dati atrasti pasaules tīmeklī saistībā ar Darījumiem jūsu lestādēs.
- **Aizdomas par ļaunprogrammatūru:** American Express ir aizdomas, ka jūs lietojat programmatūru, kas ir inficēta ar ļaunprātīgu kodu vai nav aizsargāta pret to.

TAP ir paredzēta potenciālo Kartes īpašnieka datu apdraudējumu identificēšanai.

Jums un jūsu Aptvertajām personām jāievēro šādas prasības, saņemot paziņojumu no American Express par iespējamu Kartes īpašnieka datu apdraudējumu.

- Jums ir nekavējoties jāpārskata, vai jūsu CDE nav datu drošības nepilnību, un jānovērš viss konstatētais.
  - Jūsu trešās puses piegādātājam(-iem) jāveic rūpīga jūsu CDE izpēte, ja tas ir ārpakalpojums.

- Pēc paziņojuma no American Express saņemšanas jums ir jāsniedz pārskats par veiktajiem vai plānotajiem pārskatīšanas, novērtēšanas un/vai novēršanas pasākumiem.
- Jums ir jāiesniedz atjaunināti PCI DSS validācijas dokumenti saskaņā ar Sadaļa 2, „PCI DSS Atbilstības programma (Svarīga periodiska jūsu sistēmu validācija)“.
- Nepieciešamības gadījumā ir jāpiesaista kvalificēts PCI PFI, lai pārbaudītu jūsu CDE, ja jūs vai jūsu Aptvertā persona:
  - nespēj novērst Kartes īpašnieka datu apdraudējumu saprātīgā laika periodā, ko noteica American Express, vai
  - apstiprina, ka Datu incidents ir noticis un atbilst prasībām, kas norādītas Sadaļa 3, „Datu incidentu pārvaldības pienākumi“.

Tabula A-7: TAP Neatbilstības maksa

Apraksts	1. līmeņa Tirgotājs vai 1. līmeņa Pakalpojumu sniedzējs	2. līmeņa Tirgotājs vai 2. līmeņa Pakalpojumu sniedzējs	3. līmeņa vai 4. līmeņa Tirgotājs
Ja TAP saistības nav izpildītas pirmajā termiņā, var tikt aprēķināta Neatbilstības maksa.	$25 000 USD	$5000 USD	$1000 USD
Ja TAP saistības nav izpildītas otrajā termiņā, var tikt aprēķināta Neatbilstības maksa.	$35 000 USD	$10 000 USD	$2500 USD
Ja TAP saistības nav izpildītas trešajā termiņā, var tikt aprēķināta Neatbilstības maksa. **PIEZĪME:** *Neatbilstības maksu piemērošana var turpināties līdz pienākumu izpildei vai TAP gadījuma novēršanai.*	$45 000 USD	$15 000 USD	$5000 USD

Ja jūsu TAP pienākumi nav izpildīti, American Express ir tiesības piemērot Neatbilstības maksas kumulatīvi, ieturēt maksājumus un/vai izbeigt Līgumu.

Sadaļa 6 Konfidencialitāte

American Express veiks saprātīgus pasākumus, lai ievērotu (un liktu tās aģentiem un apakšuzņēmējiem, tostarp Portāla nodrošinātājam, ievērot) jūsu ziņojumu par atbilstību, tostarp Validācijas dokumentācijas konfidencialitāti, un neatklāt Validācijas dokumentāciju nevienai trešai personai (izņemot American Express saistītās personas, aģentus, pārstāvjus, Pakalpojumu sniedzējus un apakšuzņēmējus) trīs gadus no saņemšanas dienas, izņemot to, ka šis konfidencialitātes pienākums neattiecas uz Validācijas dokumentāciju, kas:

a. jau ir zināma American Express pirms izpaušanas;

b. ir vai kļūst publiski pieejama, American Express nepārkāpjot šo punktu;

c. ir American Express tiesiski saņemta no trešās personas bez konfidencialitātes ievērošanas pienākuma;

d. ir American Express neatkarīgi izstrādāta; vai

e. ir prasīta izpaust ar tiesas, administratīvās iestādes vai valsts iestādes rīkojumu vai ar jebkuru likumu, normatīvo aktu vai regulu, vai ar tiesas pavēsti, pieprasījumu, uzaicinājumu vai citu administratīvo vai tiesisko procesu, vai ar jebkādu oficiālu vai neoficiālu izmeklēšanu, kuru veic kāda valsts aģentūra vai iestāde (tajā skaitā jebkurš regulators, inspektors, revidents vai tiesībaizsardzības aģentūra).

Sadaļa 7 Saistību atruna

AMERICAN EXPRESS AR ŠO ATSAKĀS NO JEBKURIEM UN VISIEM SKAIDRI IZTEIKTIEM, IZRIETOŠIEM, LIKUMĀ PAREDZĒTIEM VAI CITU VEIDU APLIECINĀJUMIEM, GARANTIJĀM UN SAISTĪBĀM ATTIECĪBĀ UZ

ŠO DATU DROŠĪBAS DARBĪBAS POLITIKU, PCI DSS, EMV SPECIFIKĀCIJĀM, KĀ ARĪ QSA, ASV VAI PFI (VAI JEBKURU NO VIŅIEM) IECELŠANU VAI DARBĪBU, TAJĀ SKAITĀ JEBKĀDU GARANTIJU PAR PIEMĒROTĪBU PĀRDOŠANAI VAI LIETOŠANAI KONKRĒTAM MĒRĶIM. AMERICAN EXPRESS KARŠU IZDEVĒJI NAV TREŠO PERSONU PATIESĀ LABUMA GUVĒJI SASKAŅĀ AR ŠO POLITIKU.

Sadaļa 8 Terminu saraksts

Tikai šīs *Datu drošības darbības politikas* mērķiem tiek lietotas turpmāk norādītās definīcijas, kas ir noteicošas:

1. līmeņa Pakalpojumu sniedzējs ir Pakalpojumu sniedzējs ar 2,5 miljonu vai vairāk American Express Karšu darījumu gadā; vai jebkurš Pakalpojumu sniedzējs, kuru American Express citādi uzskata par 1. līmeņa Pakalpojumu sniedzēju.

2. līmeņa Pakalpojumu sniedzējs ir Pakalpojumu sniedzējs ar mazāk nekā 2,5 miljoniem American Express Karšu darījumu gadā; vai jebkurš Pakalpojumu sniedzējs, kuru American Express neuzskata par 1. līmeņa Pakalpojumu sniedzēju.

1. līmeņa Tirgotājs ir Tirgotājs ar 2,5 miljonu vai vairāk American Express Karšu darījumiem gada laikā vai jebkurš Tirgotājs, kuru American Express citādi pieskaita 1. līmenim.

2. līmeņa Tirgotājs ir Tirgotājs, kuram ir no 50 000 līdz mazāk nekā 2,5 miljoniem American Express Karšu darījumu gadā.

3. līmeņa Tirgotājs ir Tirgotājs, kuram ir no 10 000 līdz mazāk nekā 50 000 American Express Karšu darījumu gadā.

4. līmeņa Tirgotājs ir Tirgotājs ar mazāk kā 10 000 American Express Karšu darījumiem gadā.

American Express karte vai **Karte** ir jebkura karte, konta piekļuves ierīce, maksājumu ierīce vai pakalpojums, kurā norādīts American Express vai saistītās personas nosaukums, logotips, preču zīme, pakalpojumu zīme, tirdzniecības nosaukums, cits patentēts dizains vai apzīmējums un kuru izdevis izdevējs, vai kartes konta numurs.

Apdraudētās Kartes numurs ir American Express Kartes konta numurs, kas saistīts ar Datu incidentu.

Apstiprinātais divpunktu šifrēšanas (P2PE) risinājums, kas iekļauts PCI SSC validēto risinājumu sarakstā vai kuru apstiprinājusi Maksājumu karšu nozares drošības standartu padomes (PCI SSC) Kvalificēts drošības novērtētājs (P2PE Uzņēmums).

Apstiprināts skenēšanas pakalpojumu sniedzējs (ASV) ir Uzņēmums, kuram ir piešķirta Payment Card Industry Security Standards Council, LLC licence, lai apstiprinātu noteiktu PCI DSS prasību ievērošanu, veicot interneta vides ievainojamības skenēšanu.

Aptvertās personas ir jebkuri vai visi jūsu darbinieki, aģenti, pārstāvji, apakšuzņēmēji, Starpniekiestādes, jūsu tirdzniecības punkta aprīkojuma (POS) vai sistēmas, vai maksājumu apstrādes risinājumu Pakalpojumu sniedzēji, uzņēmumi, kas saistīti ar jūsu American Express Tirgotāja kontu, un jebkura cita persona, kurai jūs saskaņā ar Līgumu varat sniegt piekļuvi Kartes īpašnieka datiem vai Sensitīviem autentifikācijas datiem (vai abiem).

Atbilstības apliecinājums (AOC) ir paziņojums par jūsu atbilstību Maksājumu karšu nozares Datu Drošības Standartam (PCI DSS) atbilstoši Payment Card Industry Security Standards Council, LLC noteiktajam veidam.

Darījums ir Maksājums, Kredīts, Naudas aizdevums (vai cita pieeja skaidrai naudai) vai bankomāta darījums, kas veikts, izmantojot Karti.

Darījuma dati ir visa American Express pieprasītā informācija, kas apliecina vienu vai vairākus Darījumus, tostarp informācija, kas iegūta tirdzniecības vietā, informācija, kas iegūta vai ģenerēta Autorizācijas un lesniegšanas laikā, kā arī Jebkura maksājuma atmaksa.

Datu incidents ir incidents, kas ietver American Express Šifrēšanas atslēgu apdraudēšanu vai vismaz vienu American Express Kartes konta numuru, kurā notiek:

- nesankcionēta piekļuve Šifrēšanas atslēgām, Kartes īpašnieka datiem vai Sensitīviem autentifikācijas datiem (vai to kombinācijai), kas tiek glabāti, apstrādāti vai pārraidīti jūsu vai jūsu lietošanai sankcionētajās

vai nodrošinātajās iekārtās, sistēmās un/vai tīklos (vai to komponentos), kā arī to nesankcionēta izmantošana;

- šādu Šifrēšanas Atslēgu, Kartes īpašnieka datu vai Sensitīvo autentifikācijas datu (vai to kombinācijas) izmantošana, kas nenotiek saskaņā ar Līgumu; un/vai
- jebkādu datu nesēju, materiālu, ierakstu vai informācijas, kas satur šādas Šifrēšanas atslēgas, Kartes īpašnieka datus vai Sensitīvos autentifikācijas datus (vai to kombināciju), iespējams vai apstiprināts zudums, zādzība vai nelikumīga piesavināšanās.

Datu incidentu gadījumu logs ir ielaušanās logs (vai līdzīgi noteikts laika periods), kas noteikts gala izmeklēšanas ziņojumā (piemēram, PFI ziņojumā), vai, ja tas zināms, līdz 365 dienām pirms pēdējā mums ziņotā Datu apdraudējumā iestaistīto potenciāli Apdraudēto Kartes numuru Paziņojuma datuma.

Divpunktu šifrēšana (P2PE) ir risinājums, kas kriptogrāfiski aizsargā konta datus no punkta, kur Tirgotājs pieņem norēķinu karti, līdz drošam atšifrēšanas punktam.

Drošības tehnoloģiju uzlabošanas programma (STEP) ir American Express programma, kurā Tirgotāji tiek mudināti izmantot tehnoloģijas, kuras uzlabo datu drošību.

EMV darījums ir integrētās shēmas kartes (dažreiz saukta arī „IC karte“, „mikroshēmas karte“, „viedkarte“, „EMV karte“ vai „ICC“) darījums, kuru veic ar IC karti, ko pieņem pārdošanas punkta (POS) terminālis ar derīgu un pašreizēju EMV tipa apstiprinājumu. EMV tipa apstiprinājumi ir pieejami vietnē www.emvco.com.

EMV specifikācijas ir EMVCo, LLC izdotas specifikācijas, kas ir pieejamas vietnē www.emvco.com.

Franšīzes devējs ir uzņēmuma īpašnieks, kurš licencē personas vai organizācijas (Franšīzes ņēmējus) izplatīt preces un/vai pakalpojumus ar īpašnieka Zīmi vai darboties, izmantojot īpašnieka Zīmi; sniedz palīdzību Franšīzes ņēmējiem viņu komercdarbības veikšanā vai ietekmē Franšīzes ņēmēja darbības veidu, kā arī pieprasa Franšīzes ņēmējiem maksas samaksu.

Franšīzes ņēmējs ir neatkarīgai personai piederoša un neatkarīgi strādājoša trešā persona (tostarp franšīzes ņēmējs, licenciāts vai nodaļa), kas nav Saistītais uzņēmums, kuram Franšīzes devējs ir licencējis izmantot franšīzi, un kas ir noslēgusi rakstveida līgumu ar Franšīzes devēju, ar kuru tā konsekventi uzrāda ārēju identifikāciju, nepārprotami identificējot sevi ar Franšīzes devēja Zīmēm, vai kas ir sabiedrības rīcībā kā Franšīzes devēja uzņēmumu grupas loceklis.

Izmeklēšanas incidenta galīgā ziņojuma veidne ir veidne, ko nodrošina PCI drošības standartu padome un kas pieejama vietnē www.pcisecuritystandards.org.

Kartes lietotājs ir fiziska vai juridiska persona, (i) kura ir noslēgusi ar izdevēju līgumu par Kartes konta izveidošanu, vai (ii) kuras vārds un uzvārds parādās uz Kartes.

Kartes Izdevējs ir jebkurš Uzņēmums (tostarp American Express un tā Saistītie uzņēmumi), ko licencējis American Express vai American Express Saistītais uzņēmums, lai izsniegtu Kartes un iesaistītos Karšu izsniegšanas uzņēmējdarbībā.

Kartes īpašnieka dati ir vismaz pilns Primārā konta numurs (PAN) vai pilns PAN kopā ar kādu no šiem: kartes īpašnieka vārds/uzvārds, derīguma termiņš un/vai pakalpojuma kods. Lai uzzinātu papildu datu elementus, skatiet Sensitīvos autentifikācijas datus, kas var tikt pārsūtīti vai apstrādāti (bet ne glabāti) kā daļa no maksājuma darījuma.

Kartes īpašnieka informācija ir informācija par American Express Kartes īpašniekiem un Karšu darījumiem, ieskaitot vārdus un uzvārdus, adreses, kartes konta numurus un kartes identifikācijas numurus (CID).

Kartes īpašnieks ir klients, kuram ir izsniegta maksājumu karte, vai jebkura fiziska persona, kurai ir tiesības izmantot maksājumu karti.

Kartes īpašnieku datu vide (CDE) ir cilvēki, procesi un tehnoloģijas, kuras uzglabā, apstrādā vai pārraida kartes īpašnieka datus vai Sensitīvos autentifikācijas datus.

Kartes numurs ir unikāls identifikācijas numurs, kuru izdevēji piešķir Kartei izsniegšanas brīdī.

Konta dati sastāv no Kartes īpašnieka datiem un/vai sensitīviem autentifikācijas datiem. Skatiet Kartes īpašnieka datus un sensitīvos autentifikācijas datus.

Kredīts ir Maksājuma summa, kuru jūs atmaksājat Kartes īpašniekiem par pirkumiem vai maksājumiem, kas veikti, izmantojot Karti.

Kredīta ieraksts ir Kredīta ieraksts, kas atbilst mūsu prasībām.

Kvalificēts drošības novērtētājs (QSA) ir Payment Card Industry Security Standards Council, LLC apstiprināta organizācija, kura apstiprina PCI DSS ievērošanu.

Līgums nozīmē Vispārīgos noteikumus, Tirgotāja noteikumus un visus pievienotos grafikus un eksponātus kopā (mūsu materiālos dažkārt saukts par Karšu pieņemšanas līgumu).

Maksājuma ieraksts ir reproducējams (papīra un elektroniskā formātā) Maksājuma ieraksts, kas atbilst mūsu prasībām un satur Kartes numuru, Darījuma datumu, summu dolāros, Apstiprinājumu, Kartes īpašnieka parakstu (ja piemērojams) un citu informāciju.

Maksājuma pieteikums ir lietots ar nozīmi, kāda tam noteikta spēkā esošajā Drošas programmatūras standarta un Drošas programmatūras dzīves cikla standarta terminu sarakstā, kas ir pieejams tīmekļa vietnē www.pcisecuritystandards.org.

Maksājums ir maksājums vai pirkums, kas veikts, izmantojot Karti.

Maksājumu karšu nozares datu drošības standarts (PCI DSS) ir Maksājumu karšu nozares datu drošības standarts, kas pieejams vietnē www.pcisecuritystandards.org.

Maksājumu karšu nozares drošības standartu padomes (PCI SSC) prasības ir standartu un prasību kopums, ks saistīts ar maksājumu karšu datu nodrošināšanu un aizsardzību, tostarp PCI DSS un PA DSS, kas pieejams tīmekļa vietnē www.pcisecuritystandards.org.

Mērķtiecīga analīzes programma ir programma, kas nodrošina potenciālo Kartes īpašnieka datu apdraudējumu agrīnu identificēšanu jūsu Kartes īpašnieku datu vidē (CDE). Skatiet Sadaļa 5, „Mērķtiecīga analīzes programma (TAP)“.

Mikroshēma ir integrēta Kartē iegulta mikroshēma, kas satur Kartes īpašnieka un konta informāciju.

Mikroshēmas ierīce ir pārdošanas punkta ierīce, kurai ir derīgs un spēkā esošs EMVCo (www.emvco.com) apstiprinājums/sertifikācija un kas spēj apstrādāt AEIPS prasībām atbilstošus Mikroshēmas karšu darījumus.

Mikroshēmas karte ir Karte, kas satur mikroshēmu un var pieprasīt PIN, lai pārbaudītu Kartes lietotāja identitāti vai mikroshēmā ietverto konta informāciju, vai abus (dažreiz mūsu materiālos saukta par „viedkarti“, „EMV karti“ vai „ICC“ jeb „integrētās shēmas karti“).

Pakalpojumu sniedzēji ir sertificētās starpniekiestādes, trešo pušu starpniekiestādes, vārteju pakalpojumu sniedzēji, POS sistēmu integratori un jebkādi citi POS sistēmu Tirgotāju pakalpojumu sniedzēji vai citi maksājumu apstrādes risinājumi vai pakalpojumi.

Pārdošanas punkta (POS) sistēma ir informācijas apstrādes sistēma vai iekārta, tajā skaitā terminālis, personālais dators, elektroniskais kases aparāts, bezkontakta nolasītājs, maksājuma platforma vai process, kuru izmanto Tirgotājs, lai saņemtu autorizācijas vai iegūtu Darījuma datus, vai arī veiktu abas darbības.

Pašnovērtējuma anketa (SAQ) ir Payment Card Industry Security Standards Council, LLC izstrādāts pašnovērtējuma rīks, kura mērķis ir novērtēt un apliecināt atbilstību PCI DSS.

Patērētājs ir definēts kā kartes īpašnieks, kas iegādājas preces, pakalpojumus vai abus.

Paziņojuma datums ir datums, kurā American Express sniedz izdevējiem gala paziņojumu par Datu incidentu. Šis datums ir atkarīgs no datuma, kad American Express saņem gala izmeklēšanas ziņojumu vai iekšējo analīzi, un American Express nosaka šo datumu pēc saviem ieskatiem.

PCI-apstiprināts nozīmē to, ka PIN ievades ierīce vai Maksājuma pieteikums (vai abi) parādās brīdī, kad tiek izmantoti PCI Security Standards Council, LLC kārtotajā apstiprināto uzņēmumu un pakalpojumu sniedzēju sarakstā, kas ir pieejams vietnē www.pcisecuritystandards.org.

PCI DSS ir Maksājumu karšu nozares datu drošības standarts, kas ir pieejams vietnē www.pcisecuritystandards.org.

PCI eksperts (PFI) ir persona, kuru apstiprinājusi Maksājumu karšu nozares drošības standartu padome, LLC, lai veiktu ekspertīzi par maksājumu Kartes datu pārkāpumu vai apdraudējumu.

PCI PIN drošības prasības ir Maksājumu karšu nozares PIN drošības prasības, kas pieejamas vietnē www.pcisecuritystandards.org.

PIN ievades ierīce ir lietota ar tādu nozīmi, kas šim terminam noteikta spēkā esošajā Maksājumu karšu nozares PIN darījumu drošības (PTS) mijiedarbības vietas (POI) modulārās drošības prasību terminu sarakstā, kas ir pieejams www.pcisecuritystandards.org.

Pircēja ierosinātas maksājuma (BIP) transakcijas ir digitālo maksājumu risinājums, kas ļauj pircējiem ātri un efektīvi plānot maksājumus piegādātājiem (saistītus ar korporatīvajām kartēm).

Portāls ir American Express izvēlētā American Express PCI programmas administratora nodrošinātā ziņošanas sistēma. Tirgotājiem un Pakalpojumu sniedzējiem ir pienākums izmantot Portālu PCI validācijas dokumentācijas iesniegšanai American Express.

Primārā konta numurs (PAN) ir lietots ar nozīmi, kas šim terminam noteikta PCI DSS terminu sarakstā.

Programma ir American Express PCI atbilstības programma.

Risku mazināšanas tehnoloģija ir tehnoloģiju risinājumi, kas uzlabo American Express Kartes lietotāja datu un Sensitīvo autentifikācijas datu drošību, kā to nosaka American Express. Lai kvalificētu tehnoloģiju kā Risku mazināšanas tehnoloģiju, jums jādemonstrē efektīva tehnoloģijas izmantošana atbilstoši tās izstrādes un paredzētajam mērķim. Daži no piemēriem: EMV, Divpunktu šifrēšana un tokenizācija.

Sensitīvi autentifikācijas dati ir ar drošību saistīta informācija, ko izmanto, lai autentificētu karšu īpašniekus un/vai autorizētu maksājumu karšu darījumus. Šī informācija ietver (bet ne tikai) karšu verifikācijas kodus, pilnus ierakstu datus (no magnētiskās joslas vai līdzvērtīgas mikroshēmas), PIN un PIN blokus.

Skenēšanas atbilstības apliecinājums (AOSC) ir paziņojums par jūsu atbilstību PCI DSS, kas pamatojas uz interneta skenēšanu Payment Card Industry Security Standards Council, LLC noteiktajā veidā.

Šifrēšanas atslēga (American Express Šifrēšanas atslēga) ir visas atslēgas, kuras tiek izmantotas konta datu apstrādē, ģenerēšanā, ielādē un/vai aizsardzībā. Tas ietver, bet ne tikai, turpmāk minēto:

- Šifrēšanas atslēgas: zonas galvenās atslēgas (ZMK) un zonas PIN atslēgas (ZPK)
- Drošās kriptogrāfijas ierīcēs izmantojamās Galvenās atslēgas: Lokālās galvenās atslēgas (LMK)
- Kartes drošības koda atslēgas (CSCK)
- PIN atslēgas: bāzes atvasinājuma atslēgas (BDK), PIN Šifrēšanas atslēga (PEK) un ZPK

Starpniekiestāde ir Tirgotāju pakalpojumu sniedzējs, kurš veic autorizācijas un iesniegšanas apstrādi American Express tīklā.

Tirgotāja līmenis ir apzīmējums, ko mēs piešķiram Tirgotājiem saistībā ar to PCI DSS atbilstības validācijas saistībām, kā aprakstīts Sadaļa 2, „PCI DSS Atbilstības programma (Svarīga periodiska jūsu sistēmu validācija)“.

Tirgotājs ir tirgotājs un visas ar to saistītās personas, kas pieņem American Express Kartes atbilstoši Līgumam ar American Express vai ar to saistītajām personām.

Tokens ir kriptogrāfiskais tokens, kas aizvieto PAN, pamatojoties uz neparedzamajai vērtībai norādīto indeksu.

Validācijas dokumentācija ir AOC, kas sniegts saistībā ar Ikgadējo klātienes drošības novērtējumu, vai SAQ, AOSC un rezultātu kopsavilkums, kas sniegts saistībā ar Tīkla skenēšanu reizi ceturksnī, vai Ikgadējā drošības tehnoloģiju uzlabojumu programmas atestācijā.

Sadaļa 9 Noderīgas tīmekļa vietnes

American Express Datu drošība: www.americanexpress.com/datasecurity

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

EMVCo: www.emvco.com