AMERICAN EXPRESS

Datasikkerhedspolitik (DSOP)

AMERICAN EXPRESS

Oversigt over Ændringer af DSOP

Ikoner

Vigtige opdateringer er opført i Tabellen Oversigt over Ændringer og står også i *DSOP* med en ændringsbjælke. En ændringsbjælke er en lodret linje, som regel i venstre margen, der identificerer tilføjet eller ændret tekst. Det er kun substantielle ændringer i *DSOP* med potentielle påvirkninger af Forhandlerens operationelle procedurer, der er indikeret med en ændringsbjælke, som vist i venstre margen.

Fjernet tekst fremhæves med et skraldespandsikon, der placeres i margenen ved siden af enhver betydelig sletning af tekst, heriblandt afsnit, tabeller, paragraffer, noter og bullets. Der refereres til fjernet tekst i denne Oversigt over Ændringer ved hjælp af afsnitsnummereringen fra den foregående udgivelse for at undgå forvirring.

Blå linjer, som grænser til afsnit indikerer regionsspecifik information.

Tabel med Oversigt over Ændringer

Vigtige opdateringer er opført i oversigten over ændringer og står også i *DSOP* med en ændringsbjælke.

Afsnit/Underafsnit	Beskrivelse af Ændring
Der er ingen ændringer i denne version.	

Afsnit 1 Introduktion til DSOP og Standarder for Beskyttelse

I kraft af vores førende position inden for forbrugerbeskyttelse har American Express en forpligtelse til at beskytte Oplysninger om Kortholdere og Følsomme Godkendelsesdata, og sørge for, at de opbevares sikkert.

Dataudslip har en negativ indflydelse på Forbrugere, Forhandlere, Serviceudbydere og Kortudstedere. Selv en enkelt hændelse kan skade en virksomheds renommé alvorligt og forhindre dens evne til at drive virksomhed på en effektiv måde. Hvis vi håndterer denne trussel i form af implementering af sikkerhedspolitikker, kan det være med til at forbedre kundens tillid, øge rentabiliteten og fremme virksomhedens renommé.

American Express ved, at vores Forhandlere og Serviceudbydere (samlet du/dig) deler vores bekymring, og kræver, at **du** som en del at dine forpligtelser opfylder bestemmelserne for datasikkerhed i den Aftale, du har indgået om at modtage (for Forhandlere) eller behandle (for Serviceudbydere) American Express®-kortet (hver især **Aftalen**), og denne Datasikkerhedspolitik (DSOP), som vi til enhver tid kan ændre. Disse krav gælder for alt udstyr samt alle systemer og netværk, hvor der opbevares, behandles eller overføres Krypteringsnøgler, oplysninger om Kortholdere eller Følsomme Godkendelsesdata (eller dem alle).

De udtryk, der er anført med stort, men ikke er defineret i aftalen, har den betydning, som er beskrevet i ordlisten til sidst i denne politik.

Datasikkerhedspolitikken (DSOP) er et omfattende sæt krav, der er designet til at beskytte Kontodata, hvor den data end opbevares, behandles eller overføres.

American Express kræver, at alle Forhandlere og Serviceudbydere skal overholde Payment Card Industry Security Standard (PCI DSS). Som en del af det krav skal du skal sørge for, at du og dine Omfattede Parter:

- Opbevar kun Oplysninger om Kortholderen med det formål at foretage American Express-korttransaktioner i henhold til og som krævet ifølge Aftalen.
- Overholder de nuværende PCI DSS- og andre PCI Security Standards Council (PCI-SSC)-krav, der gælder for din behandling, lagring eller overførsel af Krypteringsnøgler, Kortholderdata eller Følsomme Godkendelsesdata senest på ikrafttrædelsesdatoen for implementering af denne version af det gældende krav.
- Sørg for, at der anvendes PCI-godkendte produkter, når der implementeres eller erstattes teknologi til at opbevare, behandle eller overføre data.

Du skal beskytte alle American Express Betalings- og Tilgodehavendekvitteringer, der gemmes i henhold til Aftalen og i overensstemmelse med disse datasikkerhedsbestemmelser, og du må kun bruge disse kvitteringer i forbindelse med dine forpligtelser i henhold til Aftalen og skal beskytte dem i overensstemmelse hermed. Du hæfter økonomisk og på anden vis over for American Express for at sikre, at dine Omfattede Parter overholder disse datasikkerhedsbestemmelser (foruden at påvise, at dine Omfattede Parter overholder politikken i henhold til Afsnit 2, "PCI DSS-overholdelsesprogram (Vigtig Periodisk Validering af dine Systemer)", medmindre andet er angivet i dette afsnit). Du kan finde oplysninger om PCI-standarder, og hvordan man overholder deres krav, på www.pcisecuritystandards.org.

Afsnit 2 PCI DSS-overholdelsesprogram (Vigtig Periodisk Validering af dine Systemer)

For at validere under PCI DSS årligt og hver 90. dag skal du foretage dig de følgende handlinger beskrevet nedenfor, statussen for dit og dine franchisetageres udstyr, systemer og/eller netværk (og deres komponenter), hvorpå der lagres, behandles eller overføres Kortholderdata eller følsomme Godkendelsesdata.

Gennemførelsen af valideringen består af fire trin:

- Trin 1: Deltag i American Express' PCI-overholdelsesprogram ifølge nærværende politik.
- Trin 2: Forstå Kravene til dit Forhandler-/Serviceudbyderniveau og til Valideringsdokumentation.
- Trin 3: Udfyld Valideringsdokumentationen, som du skal sende til American Express.
- Trin 4: Send Valideringsdokumentationen til American Express inden for de fastsatte tidslinjer.

Trin 1: Deltag i American Express' Overholdelsesprogram i henhold til denne Politik

Niveau 1-forhandlere, Niveau 2-forhandlere og alle Serviceudbydere skal, som beskrevet nedenfor, deltage i Programmet ifølge nærværende politik. American Express kan efter eget skøn udpege specifikke Forhandlere på niveau 3 og niveau 4 til at deltage i Programmet under nærværende politik.

Forhandlere og Serviceudbydere, der skal deltage i Programmet, skal tilmelde sig Portalen, der leveres af programadministratoren, som er valgt af American Express, inden for de foreskrevne tidslinjer.

- Du skal acceptere alle rimelige vilkår og betingelser forbundet med brug af Portalen.
- Du skal tildele og give nøjagtige oplysninger for mindst én datasikkerhedskontakt i Portalen. Den påkrævede information omfatter:
  - Fulde navn
  - E-mailadresse
  - Telefonnummer
  - Fysisk postadresse
- Du skal angive opdaterede eller nye kontaktoplysninger for den tildelte datasikkerhedskontakt i Portalen, når oplysningerne ændres.
- Du skal sikre dig, at dine systemer er opdateret for at tillade tjenestekommunikation fra Portalens angivne domæne.

Din manglende angivelse eller vedligeholdelse af aktuelle datasikkerhedskontaktoplysninger, eller aktivering af e-mail-kommunikation, vil ikke påvirke vores ret til at vurdere gebyrer.

Trin 2: Forstå Kravene til dit Forhandler-/Serviceudbyderniveau og til Valideringsdokumentation

Der er fire niveauer gældende for Forhandlere og to niveauer gældende for Serviceudbydere på baggrund af mængden af dine American Express-korttransaktioner.

- For Forhandlere er dette mængden indsendt af deres Forretningssteder, der går op til det højeste American Express-forhandlerkontoniveau.*
- For Serviceudbydere er dette summen af mængden, der er indsendt af Serviceudbyderen og Enhedsserviceudbyderen, som du yder service for.

Buyer Initiated Payment- (BIP) Transaktioner medtages ikke i mængden af American Express-korttransaktioner til bestemmelse af krav til Forhandlerniveau og validering. Du vil komme ind under en af de Forhandlerniveauer, som er angivet i Tabel A-1: Forhandler- og Serviceudbyderniveauer.

* I tilfælde af Franchisegivere omfatter dette volumen fra deres Franchiselokaliteter. Franchisegivere, som giver tilladelse til, at deres Franchisetagere bruger et bestemt Point of Sale (POS) System eller en bestemt serviceudbyder, skal også levere valideringsdokumentation for de berørte Franchisetagere.

Tabel A-1: Forhandler- og Serviceudbyderniveauer

Forhandlerudbyderniveau	Årlige American Express-transaktioner
Forhandler på niveau 1	2,5 millioner American Express-korttransaktioner eller mere pr. år, eller Forhandlere, som American Express på anden vis anser for at være på niveau 1.
Forhandler på niveau 2	50.000 til færre end 2,5 millioner American Express-korttransaktioner pr. år.
Forhandler på niveau 3	10.000 til færre end 50.000 millioner American Express-korttransaktioner pr. år.
Forhandler på niveau 4	Færre end 10,000 American Express-korttransaktioner pr. år.
Serviceudbyderniveau	**Årlige American Express-transaktioner**
Serviceudbyder på niveau 1	2,5 millioner American Express-korttransaktioner eller mere pr. år, eller Serviceudbydere, som American Express på anden vis anser for at være på niveau 1.
Serviceudbyder på niveau 2	færre end 2,5 millioner American Express-korttransaktioner pr. år; eller enhver serviceudbyder, der ikke anses for niveau 1 af American Express.

Forhandleres Valideringsdokumentationskrav

Forhandlere (ikke Serviceudbydere) har fire mulige Forhandlerniveauklassifikationer. Efter fastsættelse af Forhandlerniveau fra Tabel A-1: Forhandler- og Serviceudbyderniveauer (ovenfor), se Tabel A-2: Forhandleres Valideringsdokumentation for at finde kravene til valideringsdokumentation.

Tabel A-2: Forhandleres Valideringsdokumentation

Forhandlerniveau/ Årlige American Express-Transaktioner	Overholdelsesvurderingsrapport af Attestering af Overensstemmelse (ROC AOC)	Selvvurdering Spørgeskemaattestering af overholdelse (SAQ AOC) OG Kvartalsvis Eksternt Netværk Sårbarhedsscanning (scanning)	Security Technology Enhancement Program (STEP) Attestering til kvalificerede Forhandlere
Niveau 1/ 2,5 millioner eller flere	Obligatorisk	Ikke relevant	Valgfrit med godkendelse fra American Express (erstatter ROC)
Niveau 2/ 50.000 til færre end 2,5 millioner	Valgfrit	SAQ AOC obligatorisk (medmindre en ROC AOC indsendes); scanning obligatorisk med visse SAQ-typer	Valgfrit med godkendelse fra American Express* (erstatter SAQ og netværksscanning eller ROC)
Niveau 3**/ 10.000 til færre end 50.000	Valgfrit	SAQ AOC valgfrit (obligatorisk, hvis påkrævet af American Express); scanning obligatorisk med visse SAQ-typer	Valgfrit med godkendelse fra American Express* (erstatter SAQ og netværksscanning eller ROC)
Niveau 4**/ Færre end 10.000	Valgfrit	SAQ AOC valgfrit (obligatorisk, hvis påkrævet af American Express); scanning obligatorisk med visse SAQ-typer	Valgfrit med godkendelse fra American Express* (erstatter SAQ og netværksscanning eller ROC)

* **Bemærk:** American Express PCI Team vil gennemgå anmodningen og kvalificeringen og så bekræfte, om du kvalificerer dig til STEP-programmet. Kontakt din Klientforvalter og/eller AXPPCIComplianceProgram@aexp.com for at kontrollere kvalificeringen.

**For at undgå tvivl behøver Forhandlere på niveau 3 og 4 ikke at indsende Valideringsdokumentation, medmindre dette kræves efter American Express' skøn, men skal under alle omstændigheder overholde og er ansvarlige for alle andre bestemmelser i henhold til denne Datasikkerhedspolitik.

American Express forbeholder sig retten til at verificere komplethed, nøjagtighed og hensigtsmæssighed af din PCI-valideringsdokumentation. American Express kan kræve, at du fremlægger yderligere støttedokumenter til evaluering til støtte for dette formål. Derudover har American Express ret til at kræve, at du engagerer en PCI Security Standards Council-godkendt Qualified Security Assessor (QSA) eller Kriminalteknisk efterforsker fra PCI (PFI).

Krav til Serviceudbyderens Valideringsdokumentation

Serviceudbydere (ikke Forhandlere) har to mulige Niveauklassifikationer. Efter fastsættelse af Serviceudbyderniveau fra Tabel A-1: Forhandler- og Serviceudbyderniveauer (ovenfor), se Tabel A-3: Serviceudbyderens Valideringsdokumentation for at fastsætte kravene til valideringsdokumentation.

Serviceudbydere er ikke berettiget til STEP.

Tabel A-3: Serviceudbyderens Valideringsdokumentation

Niveau	Valideringsdokumentation	Krav
1	Årlig Overholdelsesvurderingsrapport af Attestering af Overensstemmelse (ROC AOC)	Obligatorisk
2	Årlig SAQ D (Serviceudbyder) og kvartalsvis netværksscanning eller årligt Overholdelsesvurderingsrapport af Attestering af Overensstemmelse (ROC AOC), hvis det foretrækkes	Obligatorisk

Det anbefales, at serviceudbydere også overholder den supplerende PCI-validering for udpegede enheder.

Security Technology Enhancement Programme (STEP)

Forhandlere, som overholder PCI DSS, kan også, efter American Express' skøn, kvalificere sig til American Express' STEP, hvis de implementerer bestemte yderligere sikkerhedsteknologier i deres Kortbehandlingsmiljøer. STEP gælder kun, hvis Forhandleren ikke har haft en Datahændelse inden for de seneste 12 måneder, og hvis 75 % af alle Forhandlerens Korttransaktioner er foretaget ved hjælp af en kombination af følgende udvidede sikkerhedsindstillinger:

- **EMV, EMV Kontaktløs eller Digital tegnebog** – på en aktiv Chipaktiveret enhed med en gyldig og aktuel EMVCo (www.emvco.com) godkendelse/certificering og i stand til at behandle AEIPS-kompatible Chipkorttransaktioner. (Forhandlere i USA skal omfatte Kontaktløse Transaktioner)
- **Punkt-til-punkt-kryptering (P2PE)** – kommunikeret til Forhandlerens processor ved hjælp af et PCI-SSC-godkendt eller QSA-godkendt P2PE-system
- **Tokenisering** – den implementerede tokeniseringsløsning skal:
  - opfylde EMVCo-specifikationer,
  - være sikret, behandlet, opbevaret, overført og fuldstændigt administreret af en PCI-kompatibel tredjepartsserviceudbyder, og
  - Token kan ikke omvendes for at afsløre demaskerede Primære kontonumre (PAN'er) til Forhandleren.

Forhandlere, som er kvalificerede til STEP-programmet, har nedsatte krav til PCI-valideringsdokumentationen, som yderligere beskrevet i Trin 3: "Udfyld Valideringsdokumentationen, som du skal sende til American Express" nedenfor.

Trin 3: Udfyld Valideringsdokumentationen, som du skal sende til American Express

Følgende dokumenter kræves til forskellige niveauer af Forhandlere og Serviceudbydere som angivet i Tabel A-2: Forhandleres Valideringsdokumentation og Tabel A-3: Serviceudbyderens Valideringsdokumentation ovenfor.

Du skal indsende Attestering af Overensstemmelse (AOC) for den relevante vurderingstype. AOC er en erklæring om din overholdelsesstatus og skal som sådan være underskrevet og dateret af det relevante ledelsesniveau i din organisation.

Ud over AOC'en kan American Express kræve, at du fremlægger en kopi af den fulde vurdering og efter vores skøn yderligere understøttende dokumenter, der viser overholdelse af PCI DSS-kravene. Denne Valideringsdokumentation udfyldes for egen regning.

Overholdelsesvurderingsrapport af Attestering af Overensstemmelse (ROC AOC) - (årligt krav) – Rapporten for overholdelse dokumenterer resultaterne af en detaljeret undersøgelse på stedet af dit udstyr, systemer og netværk (og deres komponenter), hvor Kortholderdata eller Følsomme godkendelsesdata (eller begge dele) gemmes, behandles eller overføres. Der er to versioner: en for Forhandlere og en anden for Serviceudbydere. Overholdelsesrapporten skal udføres af:

- en QSA eller
- en Intern sikkerhedsassesor (ISA) og bekræftes af din administrerende direktør, finansdirektør, informationssikkerhedschef eller hovedforpligtede

ROC AOC'en skal være underskrevet og dateret af en QSA eller ISA og det autoriserede niveau af ledelse i din organisation og leveres til American Express mindst én gang om året.

Selvvurderingsspørgeskemaattestering af overensstemmelse (SAQ AOC) - (årligt krav) – Selv-vurderingsspørgeskema tillader selvundersøgelse af dit udstyr, systemer og netværk (og deres komponenter), hvor Kortholderdata eller Følsomme godkendelsesdata (eller begge dele) gemmes, behandles eller overføres. Der er flere versioner af SAQ. Du vil vælge en eller flere baseret på dit Kortholderdatamiljø.

SAQ'en kan udfyldes af personale i din virksomhed, der er kvalificeret til at besvare spørgsmålene nøjagtigt og grundigt, eller du kan ansætte en QSA til at hjælpe. SAQ AOC'en skal være underskrevet og dateret af det autoriserede niveau af ledelse i din organisation og leveres til American Express mindst én gang om året.

Godkendt scanningsleverandørs eksterne netværkssårbarhedsscanningsoversigt (ASV-scanning) - (90 dages krav) – En ekstern sårbarhedsscanning er en fjerntest, der hjælper med at identificere potentielle svagheder, sårbarheder og fejlkonfigurationer af internetknyttede komponenter i dit Kortholderdatamiljø (f.eks. websteder, applikationer, webservere, mailservere, offentlige domæner eller værter).

Den skal udføres af en Approved Scanning Vendor (ASV).

Hvis det kræves af SAQ, skal ASV Scan Report Attestation of Scan Compliance (AOSC) eller resumé, herunder en optælling af scannede mål, certificering af, at resultaterne opfylder PCI DSS-scanningsprocedurer og overholdelsesstatus udfyldt af ASV, indsendes til American Express mindst én gang hver 90. dag.

Hvis der indsendes en ROC AOC eller STEP, er du ikke forpligtet til at levere et AOSC- eller ASV-scanningsresumé, medmindre der specifikt anmodes om det. For at undgå tvivl er scanninger obligatoriske, hvis det kræves af den pågældende SAQ.

STEP-attestation af Valideringsdokumentation (STEP) - (Årligt krav) – STEP er kun tilgængelig for Forhandlere som opfylder kriterierne i Trin 2: "Forstå Kravene til dit Forhandler-/Serviceudbyderniveau og til Valideringsdokumentation" ovenfor. Hvis din virksomhed er kvalificeret, skal du udfylde og indsende STEP Attestation-formularen årligt til American Express. Den Årlige STEP Attestation-formular kan downloades fra Portalen. Du kan også kontakte din Klientforvalter eller skrive til American Express på AXPPCIComplianceProgram@aexp.com.

Ikke-overensstemmelse med PCI DSS - (årligt, 90-dages og/eller Ad Hoc-krav) – Hvis du ikke er kompatibel med PCI DSS, skal du indsende en oversigt over PCI-prioriteret Metodeværktøj og Attestation for overholdelse (kan downloades via PCI Security Standards Council-websitet).

Oversigten over det Prioriterede Metodeværktøj skal indeholde en afhjælpningsdato, som ikke må overskride 12 måneder efter udfyldelsen af dokumentet, for at opnå overholdelse. Du skal sende regelmæssige opdateringer til American Express med dit fremskridt mod afhjælpning af din ikke-overholdelsesstatus (Forhandlere på niveau 1, 2, 3, 4; alle Serviceudbydere). Afhjælpningshandlinger, der er nødvendige for at opnå overholdelse af PCI DSS, skal fuldføres for egen regning.

American Express opkræver ikke gebyr for overtrædelser før afhjælpningsdatoen. Iht. Tabel A-4: Gebyr for overtrædelse forbliver du ansvarlig over for American Express for alle erstastningsforpligtelser for en Datahændelse og er underlagt alle bestemmelser i denne politik.

American Express forbeholder sig retten til efter egen vurdering at opkræve gebyr for overtrædelser, hvis:

- en PCI Prioriteret Metodeskabelon ikke er blevet indsendt efter kravene, som er beskrevet i dette afsnit,

- de afhjælpningstrin, der er skitseret i den PCI Prioriterede Metodeskabelon for Overtrædelsesstatus, ikke er blevet opfyldt,
- nogen af kravene i den PCI Prioriterede Metodeskabelon for Overtrædelsesstatus, ikke er blevet opfyldt, eller
- den obligatoriske overholdelsesdokumentation ikke er blevet overleveret til American Express før den gældende frist eller efter anmodning.

Forhandlere/Serviceudbydere, der ikke overholder de krav, der er beskrevet i Trin 2: Forstå Kravene til dit Forhandler-/Serviceudbyderniveau og til Valideringsdokumentation, kan blive pålagt gebyrer, som beskrevet i Trin 4: Send Valideringsdokumentationen til American Express inden for den angivne tidsfrist.

For at undgå al tvivl er Forhandlere, som ikke overholder PCI DSS, ikke valgbare til STEP-programmet.

Trin 4: Send Valideringsdokumentationen til American Express inden for den angivne tidsfrist

Alle Forhandlere og Serviceudbydere, som skal deltage i Programmet skal sende den Valideringsdokumentationen, der er anført som "obligatorisk" i tabellerne i Trin 2: "Forstå Kravene til dit Forhandler-/Serviceudbyderniveau og til Valideringsdokumentation" til American Express inden for de gældende frister.

Du skal indsende din Valideringsdokumentation til American Express ved hjælp af Portalen leveret af Programadministratoren valgt af American Express. Ved at indsende Valideringsdokumentation udtrykker og garanterer du over for American Express, at følgende er sandt (efter bedste evne):

- Din evaluering var fuldstændig og grundig;
- PCI DSS-status er nøjagtigt repræsenteret på tidspunktet for færdiggørelsen, uanset om Attestering af overensstemmelse (AOC) PCI-prioriteret Metodeværktøj og Attestation for overholdelse (PAT) indsendes;
- Du er bemyndiget til at videregive oplysningerne deri og leverer Valideringsdokumentationen til American Express uden at krænke nogen anden parts rettigheder.

Gebyrer for Overtrædelse og Opsigelse af Aftale

American Express har ret til at opkræve gebyrer for overtrædelser og opsige Aftalen, hvis du ikke opfylder disse krav eller ikke indsender den obligatoriske valideringsdokumentation til American Express inden for den gældende tidsfrist. American Express vil forsøge at underrette datasikkerhedskontakten om gældende tidsfrister for hver årlig og kvartalsvise rapporteringsperiode.

Tabel A-4: Gebyr for overtrædelse

Beskrivelse*	Forhandler på niveau 1 eller Serviceudbyder på niveau 1	Forhandler på niveau 2 eller Serviceudbyder på niveau 2	Forhandler på niveau 3 eller niveau 4
Der vil blive fastsat et gebyr for overtrædelse, hvis valideringsdokumentationen ikke er modtaget inden den første tidsfrist.	USD $25.000	USD $5.000	USD $50
Der vil blive fastsat et ekstra gebyr for overtrædelse, hvis valideringsdokumentationen ikke er modtaget inden den anden tidsfrist.	USD $35.000	USD $10.000	USD $100
Der vil blive fastsat et ekstra gebyr for overtrædelse, hvis valideringsdokumentationen ikke er modtaget inden den tredje tidsfrist. **BEMÆRK:** Gebyrer for overtrædelse vil fortsat blive pålagt, indtil valideringsdokumentationen er indsendt.	USD $45.000	USD $15.000	USD $250

* Gebyrer for overtrædelse fastlægges modsvarende i Lokal Valuta.

* Gælder ikke i Argentina.

Hvis dine forpligtelser på PCI DSS-overholdelsesdokumentation ikke opfyldes, har American Express ret til at opkræve Gebyrer for overtrædelse kumulativt, tilbageholde betalinger og/eller annullere Aftalen.

Afsnit 3 Forpligtelser vedrørende Håndtering af Datahændelser

Du skal straks informere American Express om, og senest tooghalvfjerds (72) timer efter, at du har opdaget en Datahændelse.

Du kan informere American Express ved at kontakte American Express Enterprise Incident Response Programme (*EIRP*) gebyrfrit på +1 (888) 732-3750 eller +1 (602) 537-3021 eller ved at sende en e-mail til EIRP@aexp.com. Du skal udnævne en kontaktperson vedrørende den pågældende Datahændelse. Derudover:

- Du skal foretage en grundig teknisk undersøgelse af hver enkelt Datahændelse og øjeblikkeligt underrette American Express om alle Kompromitterede Kortnumre. American Express forbeholder sig ret til at foretage sin egen interne analyse for at identificere data, der er berørt af Datahændelsen.

For Datahændelser, der omfatter færre end 10.000 unikke Kortnumre, skal der indleveres en sammenfatning af undersøgelsen til American Express inden for ti (10) hverdage fra, at den bliver færdiggjort.

- Sammenfatninger af undersøgelser skal indeholde følgende information: sammenfatning af hændelse, beskrivelse af påvirkede miljøer, tidslinje for begivenheder, vigtige datoer, detaljer om påvirkning og

dataeksponering, inddæmnings- og afhjælpningstiltag og bekræftelse på, at der ikke er yderligere American Express-data, som er i fare.

Ved Datahændelser, der involverer 10.000 eller derover unikke Kortnumre, skal du hyre en PCI PFI med henblik på at foretage denne undersøgelse fem (5) dage efter opdagelsen af en Datahændelse.

- Den uredigerede tekniske undersøgelsesrapport skal leveres til American Express inden 10 arbejdsdage efter dens afslutning.
- Tekniske Undersøgelsesrapporter skal foretages ved hjælp af den aktuelle endelige Rapportskabelon for Teknisk Undersøgelse af Hændelse, der fås hos PCI. Rapporter fra tekniske undersøgelser skal indeholde tekniske evalueringer, rapporter om overholdelse og alle andre oplysninger i forbindelse med Datahændelsen, identificere årsagen til Datahændelsen, indeholde en bekræftelse af, at du har overholdt PCI DSS på tidspunktet for Datahændelsen; og bekræfte din evne til at forhindre Datahændelser i fremtiden ved at (i) levere en plan for afhjælpning af alle PCI DSS-mangler og (ii) ved at deltage i American Express-overholdelsesprogrammet (som beskrevet nedenfor). Såfremt American Express anmoder om det, skal du fremskaffe bekræftelse fra en Qualified Security Assessor (QSA) på, at manglerne er blevet afhjulpet.

Uanset om det strider imod de forudgående afsnit i dette Afsnit 3, "Forpligtelser vedrørende Håndtering af Datahændelser":

- American Express kan efter egen vurdering kræve, at du engagerer en PFI til at udføre en undersøgelse af en Datahændelse for Datahændelser, der involverer færre end 10.000 unikke Kortnumre, eller hvor der har været flere hændelser inden for en 12-måneders periode. Enhver sådan undersøgelse skal overholde kravene beskrevet ovenfor i dette Afsnit 3, "Forpligtelser vedrørende Håndtering af Datahændelser", og skal være afsluttet inden for den tidsramme, der kræves af American Express.
- American Express kan efter eget skøn, selv hyre en PFI til at foretage en efterforskning for enhver Datahændelse og kan opkræve omkostningerne til en sådan efterforskning af dig.

Du skal vurdere Datahændelsen i henhold til gældende love om underretning om brud på datasikkerhed globalt og, hvor det vurderes nødvendigt, underrette relevante myndigheder og påvirkede Kortmedlemmer i henhold til den slags love om underretning om brud på datasikkerhed. Hvis du fastslår, at Serviceudbyderen eller en anden entitet er ansvarlig for at rapportere Datahændelsen, skal du underrette Serviceudbyderen eller entiteten om deres pligt til at følge sin forpligtelser om rapportering i henhold til gældende love om underretning om brud på datasikkerhed. Du indvilliger i at indhente skriftlig godkendelse fra American Express, før American Express bliver henvist til eller nævnt i kommunikation med Kortmedlemmerne vedrørende Datahændelsen. Du indvilligere i at bistå American Express med at give oplysninger og afhjælpe de problemer, der måtte opstå på grund af Datahændelsen, herunder at give (samt indhente nødvendige afkald, der måtte kræves for at give) American Express alle relevante oplysninger, der bekræfter din evne til at forhindre Datahændelser i fremtiden på en måde, der er i overensstemmelse med Aftalen.

Uanset om det strider imod en eventuel fortrolighedspligt i Aftalen, har American Express ret til at videregive oplysninger om Datahændelser til American Express' Kortmedlemmer, Udstedere, andre deltagere i American Express-netværket og offentligheden generelt i henhold til Gældende lovgivning, retslig, administrativ eller lovgivningsmæssig kendelse, forordning, stævning, begæring eller anden procedure for at mindske risikoen for misbrug eller anden skade eller på anden vis i et omfang, der er relevant for driften af American Express-netværket.

Hvad skal du gøre, hvis du har en Datahændelse?

Du bedes følge disse trin, hvis du har identificeret en Datahændelse i din virksomhed.

Trin 1:
Udfyld formularen Første Meddelelse om Forhandlerens Datahændelse, og send den via e-mail til EIRP@aexp.com inden for 72 timer efter, at Datahændelsen er opdaget.

Trin 2:
Foretag en grundig undersøgelse. Dette kan indebære, at du hyrer en Kriminalteknisk efterforsker fra betalingskortindustrien (PCI).

Trin 3:
Straks indsende alle kompromitterede American Express®-kortnumre.

Trin 4:
Samarbejde med os for at hjælpe med at løse alle problemer, der måtte opstå som følge af Datahændelsen.

Se Afsnit 3, "Forpligtelser vedrørende Håndtering af Datahændelser" for at få flere oplysninger om Forpligtelser vedrørende Håndtering af Datahændelser.

Har du flere spørgsmål?

USA: (888) 732-3750 (gratisnummer)

Internationalt: +1 (602) 537-3021

EIRP@aexp.com

Afsnit 4 Erstatningspligt ved Datahændelser

Din erstatningspligt over for American Express i henhold til Aftalen ved Datahændelser er, uden at der derved gives afkald på American Express' andre rettigheder og afhjælpningsforanstaltninger, anført her i Afsnit 4, "Erstatningspligt ved Datahændelser". Ud over dine erstatningsforpligtelser (hvis nogen) kan du være underlagt et gebyr for ikke-overholdelse ved Datahændelser, som beskrevet nedenfor i dette Afsnit 4, "Erstatningspligt ved Datahændelser".

Du skal kompensere American Express med et beløb på 5 USD pr. kontonummer, for Datahændelser, der omfatter:

- 10.000 eller flere American Express-kortnumre med et af følgende:
  - Følsomme Godkendelsesdata, eller
  - Udløbsdato

American Express vil dog ikke søge skadeserstatning fra dig for en Datahændelse, der involverer:

- færre end 10.000 American Express-kortnumre, eller
- flere end 10.000 American Express-kortnumre, hvis du opfylder følgende betingelser:
  - du underrettede American Express om Datahændelsen i henhold til Afsnit 3, "Forpligtelser vedrørende Håndtering af Datahændelser",
  - du havde overholdt PCI DSS på tidspunktet for Datahændelsen (ifølge PFI's undersøgelse af Datahændelsen), og
  - Datahændelsen ikke skyldtes din eller dine Omfattede Parters ulovlige adfærd.

Uanset om det strider imod de forudgående afsnit i dette Afsnit 4, "Erstatningspligt ved Datahændelser", for enhver Datahændelse, uanset antallet af American Express-kortnumre, skal du betale American Express et gebyr for ikke-overholdelse ved Datahændelser, der dog ikke må overstige et beløb på 100.000 USD pr. Datahændelse (som bestemt af American Express efter eget skøn) i tilfælde af, at du ikke overholder alle dine forpligtelser som beskrevet i Afsnit 3, "Forpligtelser vedrørende Håndtering af Datahændelser". For at undgå tvivl må det samlede gebyr for overtrædelser for Datahændelser, vurderes for den enkelte Datahændelse ikke overstige 100.000 USD.

American Express udelukker eventuelle American Express-kortkontonumre fra deres beregning, som var involveret i et tidligere Datahændelseskrav, der er fremsat inden for de tolv (12) måneder før Anmeldelsesdatoen. Alle beregninger, som foretages af American Express via denne metode, er endelige.

I henhold til Aftalen, kan American Express fakturere dig for det fulde beløb af dine erstatningsforpligtelser for Datahændelser eller trække beløbet fra American Express-betalinger til dig (eller debitere din Bankkonto i overensstemmelse hermed).

Din erstatningspligt for Datahændelser herunder må ikke anses som værende tilfældige, indirekte, spekulative, følgemæssige, særlige, strafferetlige eller eksemplariske skader i henhold til Aftalen, forudsat at disse krav ikke omfatter skader, som vedrører mistet profit eller omsætning, tab af goodwill eller tabte forretningsmuligheder.

American Express kan efter eget skøn nedsætte erstatningspligten over for Forhandlere alene for Datahændelser, som opfylder følgende kriterier:

- De Relevante Risikoreducerende Teknologier var anvendt før Datahændelsen og var i brug i hele Perioden for Datahændelsen,
- Der blev foretaget en grundig undersøgelse i overensstemmelse med PFI-programmet (medmindre andet tidligere blev aftalt skriftligt),
- Den tekniske rapport angiver tydeligt, at de Risikoreducerende Teknologier blev brugt til at behandle, opbevare og/eller sende dataene på tidspunktet for Datahændelsen, og
- Du gemmer ikke (og gemte ikke i løbet af perioden for Datahændelsen) Følsomme Godkendelsesdata eller eventuelle Kortholderdata, som ikke er gjort ulæselige.

Hvis en nedsættelse af erstatningen er relevant, vil nedsættelsen af erstatningspligten (eksklusive eventuelle gebyrer, der ikke skal overholdes) blive bestemt som følger:

Tabel A-5: Kriterier for Nedsættelse af Erstatningspligt

Nedsættelse af Erstatningspligt	Påkrævede kriterier
Standardnedsættelse: 50 %	>75 % af det samlede antal Transaktioner, der blev behandlet via Chipaktiverede enheder[1] ELLER
	Risikoreducerende teknologi i brug på >75 % af Forhandlerlokaliteterne[2]
Øget nedsættelse: 75 % til 100 %	>75 % af alle Transaktioner, der blev behandlet via Chipaktiverede Enheder[1] OG anden Risikoreducerende Teknologi i brug på >75 % af Forhandlerlokaliteterne[2]

[1] Besluttes på baggrund af American Express' interne analyse

[2] Besluttes efter PFI-undersøgelse

- Den øgede Reduktion (75-100 %) bestemmes på baggrund af den mindste procentandel af Transaktioner, der er behandlet via Chipaktiverede Enheder OG Forhandlerlokaliteter, der anvender anden Risikonedsættende Teknologi. Eksemplerne i Tabel A-6: Øget Nedsættelse af Erstatningspligt viser beregningen bag nedsættelsen af erstatningen.
- For at kvalificere som en Risikoreducerende Teknologi, skal du udvise en effektiv udnyttelse af teknologien i overensstemmelse med dens design og tiltænkte formål.

- Procentandelen af Forhandlerlokaliteter, som anvender en Risikonedsættende Teknologi, bestemmes på baggrund af en PFI-undersøgelse.
- Nedsættelsen af erstatningspligten gælder ikke for eventuelle ikke-overholdelsesgebyrer, der skal betales i forbindelse med Datahændelsen.

Tabel A-6: Øget Nedsættelse af Erstatningspligt

Eks.	Risikonedsættende teknologier i brug	Kvalificeret	Nedsættelse
1	• 80 % af Transaktioner via Chipaktiverede enheder • 0 % forhandlerlokaliteter bruger anden Risikonedsættende teknologi	Nej	50 %: Standardnedsættelse (mindre end 75 % brug af Risikonedsættende Teknologi kvalificerer ikke til Øget Nedsættelse)[1]
2	• 80 % af Transaktioner via Chipaktiverede enheder • 77 % forhandlerlokaliteter bruger anden Risikonedsættende Teknologi	Ja	77 %: Øget Nedsættelse (på baggrund af 77 % brug af Risikonedsættende Teknologi)
3	• 93 % af Transaktioner via Chipaktiverede Enheder • 100 % forhandlerlokaliteter bruger anden Risikonedsættende Teknologi	Ja	93 %: Øget nedsættelse (på baggrund af 93 % af Transaktioner via Chipaktiverede Enheder)
4	• 40 % af Transaktioner via Chipaktiverede Enheder • 90 % forhandlerlokaliteter bruger anden Risikonedsættende Teknologi	Nej	50 %: Standardnedsættelse (mindre end 75 % af Transaktioner via Chipaktiverede Enheder kvalificerer ikke til Øget Nedsættelse)

[1] En Datahændelse, som vedrører 10.000 American Express-kortkonti, til en sats på 5 USD pr. kontonummer (10.000 x 5 USD = 50.000 USD) kan kvalificere til en nedsættelse på 50 %, hvilket nedsætter erstatningspligten fra 50.000 USD til 25.000 USD, ekskl. eventuelle ikke-overholdelsesgebyrer.

Afsnit 5 Målrettet Analyseprogram (TAP)

Udslip af kortholderdata kan være forårsaget af huller i datasikkerheden i dit Kortholderdatamiljø (CDE).

Eksempler på udslip af Kortholderdata omfatter, men er ikke begrænset til:

- **Fælles Købspunkt (CPP):** American Express-Kortmedlemmer indberetter svigagtige Transaktioner på deres Kort-konti, som identificeres, og det fastlægges, at de kommer fra køb, der er foretaget hos dit Forretningssted.
- **Kortdata fundet:** American Express Kort og Kortholderdata fundet på internettet knyttet til Transaktioner hos dine Forretningssteder.
- **Malware mistænkt:** American Express har mistanke om, at du bruger software, der er smittet med eller sårbar overfor ondsindet kode.

TAP er designet til at identificere potentielle Udslip af Kortholderdata.

Du skal selv, samt sørge for, at dine Omfattede Parter, overholder følgende krav efter underretning fra American Express om et potentielt Udslip af Kortholderdata.

- Du skal omgående gennemgå dit CDE for sikkerhedshuller og afhjælpe det, du finder.
  - Du skal få dine tredjepartsforhandlere til at gennemføre en grundig undersøgelse af dit CDE, hvis det er udliciteret.

- Du skal stille en oversigt over de handlinger, du har foretaget eller planlægger at foretage i din gennemgang, evaluering og/eller afhjælpning, når du får besked fra American Express.
- Du skal stille opdaterede PCI DSS-valideringsdokumenter til rådighed i henhold til Afsnit 2, "PCI DSS-overholdelsesprogram (Vigtig Periodisk Validering af dine Systemer)".
- Hvor det er relevant, skal du sætte en kvalificeret PCI PFI til at undersøge jeres CDE, hvis du eller den Omfattede Part:
  - Ikke kan løse Udslippet af kortholderdata inden for en rimelig periode, som fastsættes af American Express, eller
  - Bekræfter, at Datahændelsen har indtruffet og overholder de krav, som er beskrevet i Afsnit 3, "Forpligtelser vedrørende Håndtering af Datahændelser".

Tabel A-7: Gebyr for overtrædelse af TAP

Beskrivelse	Forhandler på niveau 1 eller Service-udbyder på niveau 1	Forhandler på niveau 2 eller Serviceu-dbyder på niveau 2	Forhandler på niveau 3 eller niveau 4
Der kan takseres et gebyr for overtrædelse, når TAP-forpligtelser ikke er opfyldt inden for den første tidsfrist.	USD $25.000	USD $5.000	USD $1.000
Der kan takseres et gebyr for overtrædelse, når TAP-forpligtelser ikke er opfyldt inden for den anden tidsfrist.	USD $35.000	USD $10.000	USD $2.500
Der kan takseres et gebyr for overtrædelse, når TAP-forpligtelser ikke er opfyldt inden for den tredje tidsfrist. **BEMÆRK:** *Gebyrer for ikke-overholdelse kan fortsat opkræves, indtil forpligtelserne er opfyldt, eller TAP er løst.*	USD $45.000	USD $15.000	USD $5.000

Hvis dine TAP-forpligtelser ikke opfyldes, har American Express ret til at opkræve Gebyret for overtrædelse kumulativt, tilbageholde betalinger og/eller annullere Aftalen.

Afsnit 6 Fortroligt

American Express skal tage rimelige forholdsregler til at holde (og få sine agenter og underleverandører, herunder Portaludbyderen, til at holde) dine rapporter om overholdelse, herunder valideringsdokumentationen, fortrolige og ikke videregive Valideringsdokumentationen til tredjeparter (ud over American Express' tilknyttede virksomheder, agenter, repræsentanter, Serviceudbydere og underleverandører) i en periode på tre år fra det tidspunkt, hvor de modtages, med den undtagelse, at fortrolighedspligten ikke gælder for valideringsdokumentation, der:

a. allerede var kendt af American Express inden videregivelsen,

b. er eller bliver offentligt kendt uden, at det sker på grund af American Express' misligholdelse af dette afsnit,

c. er retmæssigt modtaget fra en tredjepart af American Express uden fortrolighedspligt,

d. er udviklet uafhængigt af American Express, eller

e. skal videregives ifølge en kendelse afsagt af en domstol, styrelse eller statslig myndighed eller ifølge gældende love, regler eller bestemmelser eller stævning, begæring om fremlæggelse, tilsigelse eller andre administrative eller retslige skridt eller ifølge officiel eller uofficiel efterforskning eller undersøgelse foretaget af statsligt organ eller myndighed (herunder alle kontrolorganer, tilsynsførende styrelser, sagsbehandlende organer eller retshåndhævende myndigheder).

Afsnit 7 Ansvarsfraskrivelse

AMERICAN EXPRESS FRASKRIVER SIG HERMED ENHVER ERKLÆRING, GARANTI OG ERSTATNINGSANSVAR HVAD ANGÅR DENNE DATASIKKERHEDSPOLITIK, PCI DSS'EN, EMV- SPECIFIKATIONER SAMT FASTSÆTTELSE OG UDFØRELSE AF QSA'ER, ASV'ER ELLER PFI'ER (ELLER DEM ALLE), DET VÆRE SIG DIREKTE, INDIREKTE, LOVBESTEMT ELLER PÅ ANDEN VIS, HERUNDER ENHVER GARANTI ANGÅENDE SALGBARHED ELLER EGNETHED TIL ET BESTEMT FORMÅL. AMERICAN EXPRESS-KORTUDSTEDERE ER IKKE TREDJEPARTSMODTAGERE I HENHOLD TIL DENNE POLITIK.

Afsnit 8 Ordliste

Følgende definitioner er kun gældende og regulerende for denne *Datasikkerhedspolitik*:

Aftaler Generelle Bestemmelser, Forretningsbestemmelser og alle medfølgende tidsplaner og bilag i deres helhed (nogle gange benævnt Aftale om Accept af Kort i vores materialer).

American Express-kort, eller **Kort** er ethvert kort, en kontoadgangsenhed eller en betalingsenhed eller -tjeneste med American Express' eller en tilknyttet virksomheds navn, logo, varemærke, servicemærke, handelsnavn eller andet ejendomsretligt design eller betegnelse, og som er udstedt af en udsteder eller et kortkontonummer.

Anmeldelsestidspunktet er den dato, hvor American Express oplyser den endelige anmeldelse af Datahændelsen til udstederne. En sådan dato er betinget af American Express' modtagelse af den endelige tekniske rapport eller interne analyse og bestemmes efter American Express' eget skøn.

Attestering af overensstemmelse (AOC) er en erklæring af din status for overholdelse af PCI DSS i den form, der er udarbejdet af Payment Card Industry Security Standards Council, LLC.

Attestation of Scan Compliance (AOSC) er en erklæring af din status for overholdelse af PCI DSS baseret på en netværksscanning i den form, der er udarbejdet af Payment Card Industry Security Standards Council, LLC.

Approved Point to Point Encryption (P2PE)-løsning, der er medtaget på PCI SSC-listen over validerede løsninger eller valideret af en PCI SSC Qualified Security Assessor P2PE-virksomhed.

Approved Scanning Vendor (ASV) er en Enhed, der er kvalificeret af Payment Card Industry Security Standards Council, LLC til at validere opfyldelse af bestemte PCI DSS-krav ved at foretage sårbarhedsskanning af internetorienterede miljøer.

Behandler er en serviceudbyder til Forhandleren, som sørger for behandling af autorisation og indsendelse til American Express-netværket.

Betaling er en betaling eller et køb, der foretages med et Kort.

Betalingsapplikation har den betydning, der er angivet i den til enhver tid gældende ordliste for Secure Software Standard og Secure Software Life Cycle Standard, som findes på www.pcisecuritystandards.org.

Betalingskvittering er en reproducerbar (både på papir og elektronisk) registrering af en Betaling, som overholder vores krav og indeholder Kortnummer, Transaktionsdato, beløb i dollar, Godkendelse, Kortmedlemmets underskrift (hvis relevant) og anden information.

Buyer Initiated Payment- (BIP) Transaktioner Transaktioner er en digital betalingsløsning, der lader købere hurtigt og effektivt planlægge betalinger til leverandører (knyttet til erhvervskort).

Chip er en integreret mikrochip i Kortet, der indeholder oplysninger om Kortmedlemmet og kontoen.

Chip-Aktiveret enhed er en enhed på salgsstedet, der har en gyldig og gældende EMVCo-godkendelse/-certificering (www.emvco.com) og kan behandle Transaktioner med Chipkort i henhold til AEIPS.

Chipkort er et Kort, der indeholder en Chip, og hvor der evt. kræves en PIN-kode til verificering af kortmedlemmets identitet eller de kontooplysninger, der er på Chippen, eller begge dele (kaldes også "smartkort", "EMV-kort", "ICC" eller "integreret kredsløbskort" i vores materiale).

Datahændelse er en hændelse, som involverer lækage af American Express-krypteringsnøgler eller mindst ét American Express-kortkontonummer, hvori der er:

- uautoriseret adgang eller brug af Krypteringsnøgler, Kortholderdata eller Følsomme Godkendelsesdata (eller en kombination af disse), som er opbevaret, behandlet eller overført på dit udstyr, dine systemer og/eller dine netværk (eller dele deraf) eller brugen af denne, som du har givet tilladelse til, stillet til rådighed eller givet adgang til,
- brug af sådanne Krypteringsnøgler, Kortholderdata eller Følsomme Godkendelsesdata (eller en kombination af disse) ud over, hvad der er i overensstemmelse med Aftalen og/eller
- mistanke om eller bekræftet tab, tyveri eller misbrug af midler ved hjælp af vilkårlige medier, materialer, poster eller oplysninger, som indeholder sådanne Krypteringsnøgler, Kortholderdata eller Følsomme Godkendelsesdata (eller en kombination af disse).

Datahændelsesvindue er det vindue for indtrængen (eller en tilsvarende bestemt tidsperiode), der er angivet i den endelige kriminaltekniske rapport (f.eks. PFI-rapporten), eller hvis den er ukendt, op til 365 dage før det sidste Anmeldelsestidspunkt for potentielt Kompromitterede kortnumre, der er involveret i en Datakompromittering, der er rapporteret til os.

EMV-specifikationer er de specifikationer, der er udarbejdet af EMVCo, LLC, og som kan ses på www.emvco.com.

EMV-transaktion er en Transaktion, foretaget med et integreret kredsløbskort (kaldes også "IC-kort", "chipkort", "smartkort", "EMV-kort" eller "ICC") på en terminal på et salgssted (POS), hvor der kan benyttes et IC-kort, med en gyldig og gældende EMV-typegodkendelse. EMV-typegodkendelser kan ses på www.emvco.com.

Forbruger er defineret som en kortholder, der køber varer, ydelser eller begge dele.

Forhandler er Forhandleren og alle dennes associerede selskaber, som accepterer American Express-kort under en Aftale med American Express eller dennes associerede selskaber.

Forhandler på niveau 1 er en Forhandler med 2,5 millioner American Express-korttransaktioner eller mere pr. år eller Forhandlere, som American Express på anden vis anser for at være på niveau 1.

Forhandler på niveau 2 er en Forhandler med 50.000 til færre end 2,5 millioner American Express-korttransaktioner pr. år

Forhandler på niveau 3 er en Forhandler med 10.000 til færre end 50.000 American Express-korttransaktioner pr. år.

Forhandler på niveau 4 er en Forhandler med færre end 10.000 American Express-korttransaktioner pr. år.

Forhandlerniveau betyder den betegnelse, vi tildeler Forhandlere i forbindelse med deres PCI DSS-overholdelsesvalideringsforpligtelser, som beskrevet i Afsnit 2, "PCI DSS-overholdelsesprogram (Vigtig Periodisk Validering af dine Systemer)".

Følsomme Godkendelsesdata er sikkerhedsrelateret information, der anvendes til at bekræfte kortholderes identitet og/eller autorisere transaktioner med betalingskort. Denne information omfatter, men er ikke begrænset til, kortbekræftelseskoder, udtømmende sporingsdata (fra magnetstribe eller tilsvarende på en chip), pinkoder og pinkodespærringer.

Franchisegiver er operatøren af en virksomhed, som giver licenser til personer eller enheder (Franchisetagere) med henblik på at distribuere varer og/eller tjenester under eller ved hjælp af operatørens mærke, yder assistance til Franchisetagere i drift af deres virksomhed eller påvirker Franchisetagerens driftsmetode, og som kræver betaling via et gebyr fra Franchisetagere.

Franchisetager er en tredjepart (herunder en franchisetager, licenstager eller filial), der ejes og føres uafhængigt og ikke er et datterselskab, der har licens fra en Franchisegiver til at føre en franchise, og har indgået en skriftlig aftale med Franchisegiveren, hvor den konsekvent viser ekstern identifikation, der tydeligt identificerer sig med Franchisegiverens mærker eller udgiver sig til offentligheden som værende et medlem af Franchisegiverens virksomhedsgruppe.

Kompromitteret kortnummer er et American Express- kortkontonummer, der er relateret til en datahændelse.

Kontodata består af Kortholderdata og/eller Følsomme Godkendelsesdata. Se Kortholderdata og Følsomme Godkendelsesdata.

Kortholder er en kunde, der udstedes betaling til, eller enhver person, der er autoriseret til at bruge betalingskortet.

Kortholderdata er som minimum det fulde Primær kontonummer (PAN) for sig selv, eller fuld PAN plus alt af følgende: kortholdernavn, udløbsdato og/eller servicekode. Du kan i Følsomme Godkendelsesdata finde yderligere dataelementer, der kan blive overført eller behandlet (men ikke gemt) som en del af en betalingstransaktion.

Kortholderdatamiljø (CDE) vil sige folk, processer og teknologi, som lagrer, behandler eller transmitterer kortholderdata eller følsomme godkendelsesdata.

Kortmedlem betyder en enkeltperson eller juridisk enhed (i), der har indgået en aftale om at oprette en Kortkonto hos en udsteder, eller (ii) hvis navn står på Kortet.

Kortmedlemsoplysninger er oplysninger om American Express-kortmedlemmer og -korttransaktioner, herunder navne, adresser, kortkontonumre og kortidentifikationsnumre (CID'er).

Kortnummer er det unikke identificerende nummer, som udstederen tildeler Kortet, når det udstedes.

Kortudsteder er en entitet (herunder American Express og dennes tilknyttede virksomheder), der har licens fra American Express eller et American Express-datterselskab til at udstede kort og føre kortudstedende virksomhed.

Kriminalteknisk efterforsker fra PCI (PFI) er en enhed, der er godkendt af Payment Card Industry Security Standards Council, LLC til at foretage tekniske undersøgelser af misligholdelse eller kompromittering af betalingskortdata.

Kriminalteknisk hændelsesrapportskabelon betyder den skabelon, der er tilgængelig fra PCI Security Standards Council, og som findes på www.pcisecuritystandards.org.

Krypteringsnøgle ("American Express-krypteringsnøgle") er alle nøgler, der bruges til behandling, udfærdigelse, indlæsning og/eller beskyttelse af konto data. Dette omfatter, men er ikke begrænset til, følgende:

- Vigtige krypteringsnøgler: Zone Master Keys (ZMK'er) og Zone Pin Keys (ZPK'er)
- Masternøgler, der bruges i sikre kryptografenheder: Local Master Keys (LMK'er)
- Card Security Code Keys (CSCK'er)
- PIN-nøgler: Base Derivation Keys (BDK'er), PIN Encryption Key (PEK'er) og ZPK'er

Målrettet analyseprogram vil sige et program, som tidligt identificerer et potentielt Udslip af kortholderdata i dit Kortholderdatamiljø (CDE). Se Afsnit 5, "Målrettet Analyseprogram (TAP)".

Omfattede parter er alle jeres medarbejdere, agenter, repræsentanter, underleverandører, Behandlere, Serviceudbydere, leverandører af point-of-sale (POS)-udstyr eller -systemer eller løsninger til behandling af betalinger, Entiteter med relation til din American Express-Forhandlerkonto og andre parter, som du eventuelt giver adgang til Kortholderdata eller Følsomme Godkendelsesdata (eller begge dele) i henhold til Aftalen.

Payment Card Industry Data Security Standard (PCI DSS) er betalingskortindustriens standard for datasikkerhed, som er tilgængelig på www.pcisecuritystandards.org.

Payment Card Industry Security Standards Council- (PCI SSC) krav er det sæt standarder og krav, der er relateret til sikring og beskyttelse af betalingskortdata, herunder PCI DSS og PA DSS, og kan findes på www.pcisecuritystandards.org.

PCI DSS betyder Payment Card Industry Data Security Standard, som er tilgængelig på www.pcisecuritystandards.org.

PCI-godkendt betyder, at en PIN-Indtastningsenhed eller en betalingsapplikation (eller begge dele) på anvendelsestidspunktet er anført på listen over godkendte virksomheder og udbydere, der er udarbejdet af PCI Security Standards Council, LLC, og som er tilgængelig på www.pcisecuritystandards.org.

PCI PIN-sikkerhedskrav er betalingskortbranchens PIN- sikkerhedskrav, der kan ses på www.pcisecuritystandards.org.

PIN-indtastningsenhed har den betydning, der er anført i den gældende ordliste for Payment Card Industry PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements, om som kan findes på www.pcisecuritystandards.org.

Point of Sale (POS) System er et informationsbehandlingssystem eller -udstyr, herunder en terminal, pc, elektronisk kasseapparat, kontaktløs læser eller betalingsprogram eller -proces, som bruges af Forhandleren til at opnå godkendelser eller indsamle Transaktionsdata, eller begge dele.

Point-to-Point Encryption (P2PE) er en løsning, som beskytter kontodata kryptografisk fra det tidspunkt, hvor Forhandleren modtager betalingskortet til det sikre krypteringstidspunkt.

Portalen er rapporteringssystemet leveret af American Express PCI-programadministratoren valgt af American Express. Forhandlere og Tjenesteudbydere er forpligtet til at bruge portalen til at indsende PCI-valideringsdokumentation til American Express.

Primær kontonummer (PAN) har den betydning, det er tildelt i den på pågældende tidspunkt aktuelle Ordliste over begreber for PCI DSS.

Programmet er American Express' PCI-overholdelsesprogram.

Qualified Security Assessor (QSA) er en enhed, der er kvalificeret af Payment Card Industry Security Standards Council, LLC til at validere overholdelse af PCI DSS.

Risikonedsættende teknologi er teknologiske løsninger, der forbedre sikkerheden af American Express-kortholderdata og Følsomme Godkendelsesdata, bestemt af American Express. For at kvalificere som en Risikoreducerende Teknologi, skal du udvise en effektiv udnyttelse af teknologien i overensstemmelse med dens design og tiltænkte formål. Eksempler omfatter men er ikke begrænset til: EMV, Point to Point Encryption og generering af token.

Security Technology Enhancement Program (STEP) er det American Express-program, hvor Forhandlere opfordres til at implementere teknologier til forbedring af datasikkerheden.

Self-Assessment Questionnaire (SAQ) er et selvevalueringsredskab, der er udviklet af Payment Card Industry Security Standards Council, LLC, til evaluering og bekræftelse af overholdelse af PCI DSS.

Serviceudbydere er autoriserede behandlere, tredjepartsbehandlere, gatewayudbydere, integratorer af POS- systemer og andre udbydere til Forhandlere af POS-systemer eller andre betalingsbehandlingsløsninger eller -ydelser.

Serviceudbyder på niveau 1 er en serviceudbyder med 2,5 millioner American Express- korttransaktioner eller mere pr. år, eller Serviceudbydere, som American Express på anden vis anser for at være på niveau 1.

Serviceudbyder på niveau 2 er en Serviceudbyder med færre end 2,5 millioner American Express-korttransaktioner pr. år, eller Serviceudbyder, som American Express ikke anser for at være på niveau 1.

Tilgodehavende er den del af Transaktionen, der refunderes til Kortmedlemmer for køb eller betalinger, der foretages med Kortet.

Tilgodehavendekvittering er en registrering af Tilgodehavende, der overholder vores krav.

Token er det kryptografiske token, der erstatter PAN, baseret på et givet indeks for en uforudsigelig værdi.

Transaktion er en Betaling, Tilgodehavende, Kontant Forskud (eller anden adgang til kontanter) eller Transaktioner i hæveautomater, der foretages med et Kort.

Transaktionsdata er al information, som American Express kræver, der er bevis på en eller flere Transaktioner, herunder information, som indhentes ved et salgspunkt, information, der indhentes eller genereres under Godkendelse og Indsendelse samt Tilbageførsel.

Valideringsdokumentation er den AOC, der udfærdiges i forbindelse med Årlig sikkerhedsvurdering på stedet eller SAQ, AOSC og overordnede konklusioner af resultater i forbindelse med Kvartalsvise netværksscanninger eller årlig STEP-attestation.

Afsnit 9 Nyttige websteder

American Express-datasikkerhed: www.americanexpress.com/datasecurity

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

EMVCo: www.emvco.com