PCI-standarden

PCI DSS står för Payment Card Industry Data Security Standard. Standarden beskriver regler för den miljö (terminal/betallösning/system/nätverk) där ditt säljföretag och era leverantörer behandlar och lagrar kortdata.

De 12 kraven i PCI DSS gäller alla säljföretag

Alla säljföretag som hanterar kortdata ska uppfylla de 12 kraven som PCI DSS består av. För att ditt säljföretag ska kunna uppfylla kraven ska terminaler/betalningslösningar vara certifierade i enlighet med PA DSS och PCI PTS.

Payment Card Industry Data Security Standard (PCI DSS) beskriver kraven som alla säljföretag som överför, behandlar eller lagrar kortdata måste uppfylla. Standarden gäller för Visa och MasterCard.
PCI-DSS 12 säkerhetskrav

Implementera och upprätthåll ett säkert nätverk

Krav 1: du ska säkra att ditt säljföretag installerar och upprätthåller en brandvägg som beskyddar kortdata
Krav 2: du ska inte använda standardinställningar för lösenord till system och andra säkerhetsparametrar
Beskydda kortdata

Krav 3: du ska beskydda kortdata
Krav 4: du ska kryptera kortdata som sänds över öppna offentliga nätverk
Upprätthåll ett sårbarhetsprogram

Krav 5: du ska använda anti-virus och uppdatera det regelbundet
Krav 6: du ska utveckla och upprätthålla säkra system och applikationer löpande
Implementera en strikt åtkomstkontroll

Krav 7: du ska begränsa åtkomsten till kortdata i förhållande till verksamhetens behov och begränsa det till så få som möjligt
Krav 8: alla användare som har tillgång till era system ska ha ett unikt ID
Krav 9: du ska implementera en restriktiv hållning för fysisk tillgång till kortdata
Övervaka och testa ert nätverk regelbundet

Krav 10: du ska övervaka all tillgång till ert nätverk och kortdata
Krav 11: du ska genomföra regelbundna tester av säkerhetssystem och procedurer
Upprätthåll en informationspolicy gällande säkerhet

Krav 12: du ska upprätthålla en säkerhetspolicy