Payment Card Industry Data Security Standard (PCI DSS) ir maksājumu karšu nozares datu drošības standarts, ko veido 12 visaptverošas drošības prasības informācijas aizsardzības nodrošināšanai maksājumu karšu industrijas programmatūrai, tehnikai, uzņēmuma iekšējiem procesiem, procedūrām, IT arhitektūrai un programmatūras izstrādes procesam. Šo prasību ievērošana ir svarīga, lai palīdzētu uzņēmumiem, kas sniedz karšu maksājumu pieņemšanas pakalpojumus vai darbojas par starpniekiem to sniegšanā, proaktīvi aizsargāt klientu datus, veicot maksājumu karšu datu apstrādes procesu.

PCI DSS ir obligāts bankām, pakalpojumu sniedzējiem un uzņēmumiem, kas pieņem, apstrādā, pārraida vai glabā maksājumu karšu datus. Bankas uzņemas atbildību pret starptautiskajām maksājumu karšu organizācijām par to tirgotāju, kuru intereses tās pārstāv, atbilstību standartam.

Standartu izstrādē piedalījušās starptautisko maksājumu karšu kompānijas *Visa*, *Mastercard*, *Discover Financial Services*, *American Express* un JCB. Saskaņā ar pašlaik spēkā esošajām MC norādēm, sākot ar 2010. gada 15. decembri, 1. līmeņa tirgotājiem jāveic atbilstības PCI DSS novērtējums, ko veic vai nu sertificēta auditorkompānija, vai iekšējais auditors; 2. līmeņa tirgotājiem jāaizpilda pašnovērtējuma anketa. *Visa* norāda, ka tirgotājam līdz 2012. gada 31. decembrim jānodrošina pilnīga atbilstība PCI DSS (*Account Information Security* (AIS) *programme*).

PCI DSS nosaka prasības katram uzņēmumam atkarībā no apstrādāto transakciju skaita. Šajā tabulā sniegts katra līmeņa apraksts un norādītas veicamās drošības pārbaudes.

Līmenis	**Kritērijs**	**Prasības**	**Veicējs**
1. līmenis	Tirgotāji, kuru karšu darījumu skaits gadā pārsniedz 6 milj.	Drošības audits – reizi gadā un tīkla skenēšana – reizi ceturksnī	Sertificēts auditors veic drošības pārbaudi, kvalificēts skenēšanas speciālists veic tīkla skenēšanu.
2. līmenis	Tirgotāji, kuru karšu darījumu skaits gadā ir 1–6 milj. E-komercijas tirgotāji, kuru darījumu skaits gadā ir 150 000–6 milj.	Pašnovērtējuma anketa – reizi gadā un tīkla skenēšana – reizi ceturksnī	Tirgotājs aizpilda pašnovērtējuma anketu un iesniedz to bankai; neatkarīgs kvalificēts skenēšanas speciālists veic tīkla skenēšanu.
3. līmenis	E-komercijas tirgotāji, kuru darījumu skaits gadā ir 20 000–150 000.	Pašnovērtējuma anketa – reizi gadā un tīkla skenēšana – reizi ceturksnī	Tirgotājs aizpilda pašnovērtējuma anketu un iesniedz to bankai; neatkarīgs kvalificēts skenēšanas speciālists veic tīkla skenēšanu.
4. līmenis	Visi citi tirgotāji	Ieteicams aizpildīt pašnovērtējuma anketu; ieteicams veikt tīkla skenēšanu reizi gadā	Tirgotājs aizpilda pašnovērtējuma anketu; neatkarīgs kvalificēts skenēšanas speciālists veic

tīkla skenēšanu.
Pat ja pašnovērtējuma anketas aizpildīšana ir ieteicama, prasību ievērošana ir obligāta.

Tirgotāji, kas apkalpo maksājumu kartes, informāciju par atbilstības līmeni, PCI DSS ieviešanas procesu, nepieciešamību modernizēt karšu apkalpošanas sistēmas infrastruktūru un/vai datu kriptēšanas mehānismu, kā arī pārbaudīt uzņēmuma procedūru atbilstību PCI DSS var saņemt no pieņēmējbankas.

Pašnovērtējuma anketa:
https://www.pcisecuritystandards.org/saq/instructions_dss.shtml#instructions

Uzņēmuma iekšējā audita gaitā jāpārliecinās par 12 PCI DSS prasību ievērošanu. Katrai prasībai ir izstrādāta papildu jautājumu kopa (www.pcisecuritystandards.org), kas palīdz pārliecināties vai prasības ir ievērotas.

- Sertificēts inspektors (kvalificēts drošības novērtētājs (*Qualified Security Assessor*; QSA)) uz vietas veic drošības pārbaudi.
- Kvalificēts tīklu skenēšanas speciālists veic tīkla skenēšanu (gadījumos, kad tirgotājs lieto internetu).
- Veic uzņēmuma iekšējo drošības auditu, aizpildot pašnovērtējuma anketu (*Self Assessment Questionnaire*; SAQ).

Par PCI DSS atbilstības termiņiem tirgotājam nepieciešams vienoties ar pieņēmējbanku, iesniedzot standarta atbilstības sasniegšanas plānu, kurā norādītas veicamās darbības un termiņi.

PCI DSS prasības

Jāizveido un jāuztur drošs tīkls
1. Jāuzstāda un jāuztur ugunsmūra konfigurācija karšu lietotāju datu aizsardzībai.
2. Nedrīkst izmantot aparatūras vai programmatūras pārdevēja uzstādītās noklusējuma sistēmas paroles un citus drošības parametrus.

Jāaizsargā karšu lietotāju dati
3. Jāaizsargā karšu lietotāju dati.
4. Pārraidot karšu lietotāju datus atvērtos publiskos tīklos, tie jāšifrē.

Jālieto t.s. vājo vietu kontroles programma
5. Jālieto un regulāri jāatjaunina antivīrusu programmatūra.
6. Jāizstrādā un jāuztur drošības sistēmas un programmatūras.

Jāievieš strikti piekļuves kontroles pasākumi
7. Piekļuve karšu lietotāju datiem jāatļauj tikai tad, ja pastāv attiecīga ar uzņēmējdarbību saistīta nepieciešamība.
8. Jāpiešķir unikāla identifikācija ikvienam darbiniekam, kuram ir pieeja datoram.
9. Jāierobežo fiziska piekļuve karšu lietotāju datiem.

Tīkli regulāri jākontrolē un jāpārbauda
10. Jāseko līdzi un jākontrolē visa piekļuve tīkla resursiem un karšu lietotāju datiem.

11. Regulāri jāpārbauda drošības sistēmas un drošības procesi.

Jāīsteno informācijas drošības politika
12. Jāīsteno informācijas drošības politika, lai ikviens uzņēmuma darbinieks izprastu savu lomu datu aizsardzībā.

Noderīgas adreses
www.pcisecuritystandards.org
http://pcidssfaq.org/forum/
https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf