# PCI DSS

## 3. Protect stored cardholder data

* **3.1. Svesti podatke koji se skladište na minimum** – u bazi čuvamo samo ono što je neophodno
* **3.2. Podatke za autentifikaciju ne treba čuvati nakon autorizacije** – prilikom autorizacije koristimo JSON Web Tokene koji u sebi sadrže id korisnika i njegovu ulogu, takođe password i username posle autorizacije ne čuvamo nigde.
* **3.3. Ceo PAN ne sme da se prikaže** – sakriveni drugih 6 brojeva, na frontu u logovima, svugde gde se prikazuje

## 4. Encrypt transmission of cardholder data across open, public networks

* **4.1. Koristiti bezbedonosne protokole, da bi se zaštitili osetljivi podaci prilikom prenosa** – svuda se koristi HTTPS, implementirani sertifikati
* **4.2. Nezaštićen PAN broj ne sme da se šalje preko platformi za razmenu poruka**

## 6. Develop and maintain secure szstems and applications

* **6.3. Razvojno/test okruženje odvojiti od produkcije; podela dužnosti, ne koristiti prave PAN brojeve** – ne koristimo prave PAN brojeve
* **6.4. Best practices –** Clean code

## 7. Restrict access to cardholder data by business need to know

* **7.1. Ograničiti pristup komponentama sistema i podacima** – urađena autentifikacija i autorizacija
* **7.2. Smernice za kontrolu pristupa**

## 8. Identify and authenticate access to system components

* **8.1. Definisati i implementirati procedure za pravilno upravljanje korisnicima koji nisu potrošači i administratorima koji ne koriste sve komponente sistema** – određene funkcionalnosti dodeljene određenim ulogama
* **8.2. Najmanje jedan mehanizam za potvrdu identiteta** – username i password
* **8.5. Ne koristiti grupne, deljene ili generičke IDs, lozinke** – svi objekti u bazi imaju jedinstvene ID-eve, takođe korisnici pored ID imaju i jedinstven username. Lozinke korisnici unose sami prilikom registracije.
* **8.6. Mehanizam za potvrdu identiteta dodeliti pojedinačnom nalogu**
* **8.7. Svaki pristup bazi podataka treba da bude ograničen** – pristup podacima u bazi je dozvoljen korisnicima na osnovu uloge u sistemu.

## 10. Track and monitor all access to network resources and cardholder data

* **10.1. Postupak za povezivanje svih pristupa komponentama sa pojedinačnim korisnikom** – svaki proizvod, kurs, konferencija, itd. poseduje u sebi kupca koji je kreirao, takođe transakcije poseduju korisnika koji je otpočeo transakciju…
* **10.2. Mehanizam za praćenje svih događaja** – koristi se struktuirano logovanje
* **10.3. Za svaki događaj sačuvati: tip događaja, datum i vreme, izvor**
* **10.4. Sinhronizacija vremena**
* **10.5. Review logova** – svi logovi se čuvaju u bazi
* **10.6. Čuvati istoriju** – čuvamo sve bitne podatke, kao što su npr. sve transakcije bile uspešne ili ne

## 11. Regularly test security systems and processes