PCI DSS Стандард

1. **BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS**
   1. **Install and maintain a firewall configuration to protect cardholder data**Захтев није могуће испоштовати у пројекту.
   2. **Do not use vendor-supplied defaults for system passwords and other security parameters**Захтев није могуће испоштовати у пројекту.
2. **PROTECT CARDHOLDER DATA**
   1. **Protect stored cardholder data**

У оквиру ПСП-а не чувају се директни подаци о картици, већ само о њеном власнику, тј. они који се потребни за успостављање комуникације између ПСП-а и банке. Читав ПАН број се нигде не приказује и шифрује се у бази.

* 1. **Encrypt transmission of cardholder data across open, public networks**ПАН број се не шаље ни преко једне платформе за размену порука.

1. **MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM**
   1. **Protect all systems against malware and regularly update anti-virus software or programs**

Захтев није могуће испоштовати у пројекту.

* 1. **Develop and maintain secure systems and applications**

Зависности које постоје у систему су скрениране помоћу Snyk алата и откривене су оне које поседују рањивости.

1. **IMPLEMENT STRONG ACCESS CONTROL MEASURES**
   1. **Restrict access to cardholder data by business need to know**

Ограничење приступа је имплементирано помоћу RBAC модела.

* 1. **Identify and authenticate access to system component**

Сваки користик има свој ID број који га јединствено одређује. Имплементирана је двострука потврда идентитета тако да корисник приликом регистрације добија QR код који треба да скенира и број који добије треба увек да уноси заједно са email-ом и лозинком када се пријављује на систем. Тај број се мења на сваких 30 секунди. Поред тога, приликом регистрације мора изабрати лозинку такву да има најмање 8 цифара, бар 1 велико слово, 1 цифру и 1 специјални карактер. Групне и генеричке лозинке се не користе нигде.

* 1. **Restrict physical access to cardholder data**

Захтев није могуће испоштовати у пројекту.

1. **REGULARLY MONITOR AND TEST NETWORK**
   1. **Track and monitor all access to network resources and cardholder data**

Систем поседује механизам за логовање. Логови бележе све битне догађаје у систему и чувају се у посебним фајловима за сваки сервис.

* 1. **Regularly test security systems and processes**

Извршено је пенетрационо тестирање система.

1. **MAINTAIN AN INFORMATION SECURITY POLICY**
   1. **Maintain a policy that addresses information security for all personnel**

Захтев није могуће испоштовати у пројекту.