



# PCI DSS COMPLIANCE

Payment Card Industry Data Security Standard (PCI DSS) compliance is a set of policies and procedures developed to protect credit, debit and cash card transactions and prevent misuse of cardholder's personal information. It is a requirement for all card companies.

## PCI DSS COMPLIANCE CHECKLIST

### **Build and Maintain a Secure Network**

- Install and maintain a firewall to protect cardholder data
- Not use vendor-supplied defaults for system passwords and other security parameters

### **Protect Cardholder Data**

- Protect stored cardholder data
- Encrypt transmissions of cardholder data across open, public networks

### **Vulnerability Management Program**

- Utilize regularly updated antivirus software
- Develop and maintain secure systems and applications

### **Access Control Measures**

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person
- Restrict physical access to cardholder data

### **Monitor and Test Networks Regularly**

- Track and monitor all access to network resources and cardholder's data
- Test security system and processes regularly

### **Maintain an Information Security Policy**

- Develop and maintain a policy to address information security