11.4 PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organisations that handle cardholder information for the major credit and debit cards such as VISA and MasterCard. This industry regulation has several goals which most importantly are listed below:

1.1 Requirement: All merchants must protect cardholder information by installing a firewall and router system. Installing a firewall system provides control over the person who can access an organisation’s network and a router is a device that connects networks, which is therefore, PCI compliant.

Program the standards of firewall and router to:

1. Perform testing when configurations change

2. Identify all connections to cardholder information

3. Review configuration rules every six months

Configure firewall to prohibit unauthorised access from networks and hosts and deny direct public access to any information about the cardholder. Additionally, install firewall software on all computers that access the organisation’s PCI compliance network.

1.2 Requirement: Change all default passwords. Default passwords provided when first setting up software are discernible and can be easily discovered by hackers to access sensitive information.

2.1 Requirement: Cardholder data is any personal information about the cardholder that is found on the payment card and can never be saved by a merchant. This includes preserving encrypted authentication data after authorization. Merchants can only display the maximum of the first six and last four digits of the primary account number (PAN). If a merchant stores PAN, ensure that the data is secure by saving it in a cryptographic form.

2.2 Requirement: It is required that all information is encrypted when transmitting the data across public networks, such as the Internet, to prevent criminals from stealing the personal information during the process.

3.1 Requirement: Computer viruses make their way onto computers in many ways, but mainly through e-mail and other online activities.

The viruses compromise the security of personal cardholder information on a merchant’s computer, and therefore antivirus software must be present on all computers associated on the network.

3.2 Requirement: In addition to antivirus software, computers are also susceptible to a breach in the applications and systems installed on the computer. Merchants must install vendor-provided security patches within a month of their release to avoid exposing cardholder data. Security alert programs, scanning services, or software may be used to signal the merchant of any vulnerable information.

4.1 Requirement: As a merchant, you must limit the accessibility of cardholder information. Install passwords and other security measurements to limit employees’ access to cardholder data. Only employees who must access the information to complete their job are allowed to access the information.

4.2 Requirement: In order to trace employees’ activities when accessing sensitive information, assign each user an unreadable password used to access the cardholder data.

4.3 Requirement: Monitor the physical access to cardholder data; do not allow unauthorised persons the opportunity to retrieve the information by securing printed information as well as digital. Destroy all outdated cardholder information. Maintain a visitor log and save the log for at least three months.

5.1 Requirement: Keep system activity logs that trace all activity and review daily. The information stored in the logs is useful in the event of a security breach to trace employee activities and locate the source of the violation. Record entries reflect at a minimum: the user, event, date and time, success or failure signal, source of the affected data, and the system component.

5.2 Requirement: Each quarter, use a wireless analyser to check for wireless access points to prevent unauthorised access. Also, scan internal and external networks to identify any possible vulnerable areas in the system. Install software to recognise any modification by unauthorised personnel. Additionally, ensure that all IDS/IPS engines are up to date.

If you process credit cards, it is imperative that you comply with this standard.