Payment Card Industry Data Security Standard Policy

1 Purpose

The Payment Card Industry Data Security Standard (PCI DSS) is a set of guidelines developed by MasterCard, Visa, American Express, Discover and JCB International to assist merchants in preventing payment card fraud and to improve security around processing and storing payment card details. Any company processing, storing or transmitting the above branded payment card numbers must be PCI DSS compliant or they risk losing the ability to process these payments.

Coffs Harbour City Council (Council) is required to be compliant with the PCI DSS. Non-compliance can result in fines to merchants of at least $10,000 per month and $500,000 per card brand (e.g. Visa, MasterCard) if there is a data breach. Annual verification of compliance must be supplied to any banking institution that provides Council with the means to accept the abovementioned card payments.

2 Policy

Council is required to comply with the PCI DSS in order to process payment utilising credit/debit cards. Compliance is overseen by our banking partner and enforced by the payment card brand (Visa, Mastercard etc.).

The PCI DSS is a global set of security best practices which when implemented correctly, will assist Council in protecting our systems and help maintain the trust of our customers.

The requirements of the Standard and therefore this policy are based on six elements and twelve requirements:

- Build and Maintain a Secure Network
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Requirement 5: Use and regularly update anti-virus software
  - Requirement 6: Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Assign a unique ID to each person with computer access
  - Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes
- Maintain an Information Security Policy
  - Requirement 12: Maintain a policy that addresses information security

Non-compliance can bring about suspension of merchant accounts, fines/penalties from the payment card industry and providers. Substantial fines can apply to the following:

- per data security breach
- per day for non-compliance with published standards
- liability for all fraud losses incurred from compromised account numbers
- liability for the cost of re-issuing cards associated with the compromise, and
- suspension of merchant accounts resulting in the inability to accept credit card payments.

3 Definitions

N/A

4 Key Responsibilities

Group Leader Business Systems is responsible for the implementation and maintenance of this Policy.

5 References

- Information Security and Management Policy
- Payment Card Industry Data Security Standard Procedure

6 Details of Approval and revision

- **Approval date:** 6/12/2018
- **Responsible Group:** Business Systems Group
- **Responsible Section:** N/A
- **Superseded policies/procedures: N/A**
- **Next review date:** 31/08/2021

Table of amendments

Amendment	Authoriser	Approval ref	Date