TEG Guidelines for all computer systems handling credit card numbers.

Document Information

Version Number	1.0
Last Update	15/10/2022
Author	Matthew Coutts
File Name	TEG Guidelines for all computer systems handling credit card numbers.
Document Title	TEG Guidelines for all computer systems handling credit card numbers.
Document Owner (Role Position)	Global Head of Enterprise Technology, Risk and Cyber Security
Responsible Executive (Role Position)	Chief Technology Officer

Document Revision History

Version	Issue Date	Author	Comments	Approved By
1.0	20/10/2022	Matthew Coutts		Matthew Coutts

Document Approval and Authorisation by Senior Management

Version	Issued Date	Date Last Reviewed	Approver
1.0	20/10/2022	20/10/2022	Matthew Coutts

I. Introduction

To maintain compliance with requirements imposed by the Payment Card Industry Data Security Standard (PCI-DSS), TEG entities processing credit card payments must take appropriate measures to prevent the loss or disclosure of customer information including credit card numbers. Failure to protect the privacy of our customers may result in financial loss for many customers, fines imposed on the company, suspension of credit card processing privileges and damage to the reputation of the company. This document provides guidelines for all computer systems handling credit card numbers at TEG.

II. Guidelines

A. System Security Requirement

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications Implement
7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel
13. All credit card data should be tokenised.

B. Connectivity Security Requirement (Wired/Wireless)

1. A network-based firewall preventing inappropriate/unauthorized access from outside the business unit or specific authorized computers.
2. An intrusion detection system (IDS) that monitors for unauthorized access attempts.
3. Continuous monitoring for network-based firewall and IDS systems for potential penetrations.
4. Specific authorization for wireless connections. All wireless connections must be approved and audited by Technology Services before being implemented.
5. All data transfers and administrative access must be in an encrypted channel (e.g. TLS v1.2, SSH, IPSEC).

C. Credit card number storage requirement

1. It is prohibited to store sensitive cardholder data [i.e., full account number, expiration date, PIN, and card validation value] in any Company system and/or departmental server, third-party software, personal computer, cash register system,

e-mail account, portable electronic device (including, but not limited to, laptop, flash drive, floppy disc, CD, PDA, and external or portable hard drive), or on paper.
2. All credit card data in our point of sale systems must be tokenised.
3. Employees shall not disclose or acquire any information concerning a cardholder's account without the cardholder's consent.
4. The entire credit card number must not be printed on either the merchant copy or customer copy of any receipts or reports.
5. All media used for credit card numbers must be destroyed when retired from use.
6. Any paper receipts stored by merchants must adhere to the PCI DSS, especially requirement 9 regarding physical security.

D. Physical Security Requirement

1. The server must be in one of Technology Services secured data centers.
2. All access to servers by anyone except employees specifically approved for access to the cardholder systems must be escorted continuously.

III. Definitions

Cardholder Data: Credit card numbers (in full or in part)

Encryption: Is the process of encoding messages or information in such a way that only authorized parties can read it.

Firewall: A network device or host-based software implementation designed to restrict network access to a computer.

Hashing: The process used to map digital data of arbitrary size to digital data of fixed size.

Intrusion Detection System (IDS): A network monitoring device for recognition of attempts to compromise monitored systems.

Payment Card Industry Data Security Standard (PCI-DSS) : The unified standard data protection program mandated by VISA, MasterCard, American Express, Diners Club, Discover and JCB.

Site Data Protection Program (SDP): The formal data protection program mandated by MasterCard.

IV. References

- Payment Card Industry Data Security Standard v3.1 (PCI-DSS v3.2)
- MasterCard Site Data Protection Program (SDP)