PCI DSS - Incident Response Policy

1.Overview

An incident may be anything which affects or has the potential to affect the proper processing of data in accordance with Gemporia's business objectives and policies. It may be the result of a deliberate attack or may be accidental in its origin. The scale of incidents may vary greatly from minor inconvenience to threatening the organisation's future and there needs to be a corresponding range of possible responses.

Many of Gemporia's PCI DSS policies are concerned with preventing or detecting incidents; this policy is concerned with responding to an incident once identified through containment, eradication and recovery. This policy contributes towards compliance with PCI Data Security Standard v3.0 Requirement 12.

2.Responsibility for Maintenance

The Gemporia IT Director is responsible for ensuring that this document is kept current for the purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives. The document must be reviewed and updated at least annually with the updated version rolled out to all concerned personnel.

3.Scope

This document applies to the people, processes and technology that store, process or transmits cardholder data or sensitive authentication data, including systems that produce logging information and any connected system components. This includes contractors, vendors and any other personnel that have may have an impact on the cardholder data environment.

4.Policy Statement

Gemporia will have a documented Incident Response Plan and procedures for responding to a range of Incidents. These shall include those mentioned in the PCI DSS including, but not limited to:

- Breach of physical security including theft
- Unauthorised changes to system (hardware or software) configurations
- Loss of cardholder data
- Unauthorised access to the cardholder data environment
- Unauthorised wireless access point
- Attack by virus or other malware
- Discovery of unauthorized wireless hardware
- Unwanted disruption or denial of services
- Unacceptable use of Internet or e-mail

1. The Incident Response Plan shall include the incident response procedures required by the payment card brands
2. Roles and responsibilities for responding to incidents shall be as defined in the Roles and Responsibilities Policy with 27×7 availability
3. Incidents involving loss of or unauthorised access to cardholder data shall be notified to Gemporia's payment card acquirer, the card brands and other regulatory and law enforcement bodies as required
4. Incident response procedures shall include escalation procedures
5. Incident response procedures shall include business recovery and continuity procedures
6. Incident response procedures shall be tested annually using a combination of walkthrough, desk top, simulation and full operation testing
7. All personnel with incident response responsibilities shall have periodic training
8. The Incident Response Plan will include the requirement to monitor and respond to alerts including the detection of unauthorised wireless access points
9. Security awareness training for all personnel shall include the actions to take if staff become aware of a security incident
10. The Incident Response Plan shall be updated in response to lessons learned from actual incidents, tests and industry developments
11. The incident response plan shall take the Business Continuity Plan into account

5.Glossary

The purpose of the following glossary is to communicate the meaning of specific PCI DSS terminology used in this document. The official PCI DSS Glossary issued by the Payment Card Industry Payment Security Standards Council has been the source of the definitions used below.

Cardholder Data: At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code. See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

Cardholder Data Environment (CDE): The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.

System Components: Any network component, server, or application included in or connected to the cardholder data environment.

From:
https://techdocs.amber.cx/ - **Gemporia Wiki**

Permanent link:
https://techdocs.amber.cx/policies/incident_response

Last update: **2019/01/14 19:31**