Incident Response Procedure

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 procedure is aimed at defining the process to be followed once an incident has been identified or reported. This procedure is aimed to support the PCI DSS Incident Response Policy.

Scope

This document applies to all the assets that are covered as per the Gemporia’s PCI DSS Incident Response Policy.

Procedure

It is often difficult to detect when a system has been attacked or an intrusion has taken place. Distinguishing normal events from those that are related to an attack or intrusion is a critical part of maintaining a secure payment processing environment. A security breaches come in many different forms and, while detecting them may be challenging, there are certain signs that tend to appear when a security breach has occurred:

- Unknown or unexpected outgoing internet traffic from the payment card environment
- Presence of unexpected IP address on the CDE network
- Unknown or unexpected network traffic from call center to head office/ data centres
- Failed login attempts in system authentication and event logs
- Systems rebooting, shutting down or being inaccessible for unknown reasons
- An increase in the number of generated logs
- Discovery of unexpected wireless hardware

The following steps must be taken at the identification of an incident affecting the cardholder environment and any interfaces that may have an immediate impact to Gemporia’s ability to process payments in a secure manner.

1. Immediately take steps to contain the incident and to limit the exposure. Measures must be taken to limit data loss, if any seems to occur. In case of doubt, please reach out to your immediate supervisor or IT Help Desk for further clarification.
2. To preserve evidence and facilitate investigation, the following steps shall be taken (as appropriate)
    1. Do not access or alter compromised system(s)
    2. Do not turn off/ shut down the compromised system. Instead isolate the system from the

network (ie unplug the network cable)
    3. Preserve logs
    4. Keep a log of all actions taken
    5. If Wireless networks were identified to be part of the incident, disable the wireless connection on the device (if possible)
    6. Be on high alert for any suspicious activities
3. Alert all necessary parties immediately:
    1. Your internal incidents response team/ line manager/ supervisor
    2. Notify the appropriate law enforcement agency (if appropriate)
    3. Speak with legal representation, if applicable, to determine if any further parties should be informed
    4. If required, contact your merchant bank/ acquirer/ service provider/ vendor

Incident Response Plan

The following steps will be taken by the staff identifying the incident

1. The person who identifies an incident/ issue will contact the IT Help Desk on 6138 with the following details
    1. Name of the person reporting
    2. Type of Incident
    3. Summary
    4. Perceived Impact
    5. Does it affect a customer?
2. The IT helpdesk staff based on the incident and the perceived impact will try to solve the issue, if it’s within their remit. Else they will follow the IT escalation matrix in case of an IT issue. If the incident reported impacts the payment card infrastructure/ process, the IT helpdesk will refer to their contact matrix and inform the Incident Response Manager. It could be either be the IT Manager or IT Director.
3. The Incident Response Manager will then conduct an impact assessment based on the incident and the amount of information available. He may choose to contact the person who reported the incident for further clarifications. Based on the impact assessment, a decision will be taken as to whom to involve to deal with the incident. Based on the nature of the incident, staff from various teams or vendors could be involved in the incident management.
4. If the incident involves the Cardholder Data the Acquirer must be immediately informed and their incident strategy run in parallel with Gemporia’s own strategy. This is to be done as soon as possible but at most within 10 days.
5. Upon confirmation of a breach, inform the Police and obtain a crime reference number, to be used with all further documentation
6. The management will be informed of the outcome of the incident based on the criticality of the event with management inputs taken as necessary. The team managing the incident will provide regular update to the management about the progress of the incident.
7. Once the incident has been contained, a decision will be taken as to if a formal investigation is required. An external party could be involved if required for use of forensic tools and techniques to better understand the issue.
8. The Incident Response Management can choose to inform those affected and the concerned external agencies as required.
9. Once the factors which lead to the incident has been evaluated and analysed, further actions could be agreed to fix the incident. All actions must be approved by the necessary stakeholder

before it gets implemented. External third party help may be procured based on the incident, if necessary. This may involve restoring data from backup media, replacing compromised software and hardware or installing additional hardware or software to rectify issues.
10. Document the lessons learnt from the incident and review the solution to prevent the reoccurrence of the incident.

Contact Details

Description	Link
Visa Europe	VisaEurope.com
Mastercard Europe	Mastercard.us
American Express	AmericanExpress.com

Conclusion

This document provides the essentials for managing incidents within Gemporia's PCI DSS scope. Further documents/ templates could be created as necessary to capture the incident details and for reporting these. This process could also be extended to other relevant parts of the business as seen necessary.