D

CABINET – 5 FEBRUARY 2014. PORTFOLIO: FINANCE AND EFFICIENCY

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) POLICY

1. INTRODUCTION

1.1 The purpose of this report is to introduce a new policy which is required to maintain the Council's compliance with PCI DSS.

2. PCI DSS POLICY AND INCIDENT PLAN

2.1 Following the internal audit of the Council's compliance against the external card standards, PCI DSS, it was identified that the Council did not have the required policy in place to fully comply with the standards.

2.2 A new policy is attached within Appendix 1. The policy has been reviewed by the ICT Security Officer and Head of ICT. The incident plan has been aligned to the Council's existing security incident plan.

2.3 The policy will apply to all officers who are involved in any part of the card processing systems.

2.4 The policy will formalise procedures that are widely already in place. There are no elements of the policy which change any existing work programs.

3. FINANCIAL IMPLICATIONS & CRIME AND DISORDER IMPLICATIONS

3.1 There are no direct financial implications arising from this report, however an inadequate policy may result in inappropriate card processing. Non compliance with these card standards may result in fines or the withdrawal of card facilities which would impact on income collection.

4. ENVIRONMENTAL MATTERS & EQUALITY AND DIVERSITY IMPLICATIONS

4.1 There are no matters arising directly from this report.

5. PORTFOLIO HOLDER'S COMMENTS

5.1 The Portfolio Holder supports the recommendation below.

6.0 RECOMMENDATION

6.1 That the policy be recommended for approval. The policy be added to Forestnet and communicated to all relevant Officers.

For Further Information Please Contact:
Lucinda Upton
Internal Audit Manager
Tel: (023) 8028 5588
E-mail: lucinda.upton@nfdc.gov.uk

Background Papers:
Internal Audit PCI DSS report

Appendix 1

PCI DSS Policy

Introduction

All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card processing activities must be conducted as described herein and in accordance with the standards and procedures listed in the Related Documents section of this Policy. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.
This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

Applicability

This policy applies to all employees: full-time and part-time, temporary and personnel, and contractors and consultants who are "resident" on site. Relevant sections of this policy apply to vendors, off-site contractors, and business partners.

Configuration standards

Configuration standards must include:

- updating of anti-virus software and definitions
- provision for installation of all relevant new security patches within one month
- prohibition of group and shared passwords

Distribution, maintenance, and storage

Distribution, maintenance, and storage of media containing cardholder data, must be controlled, including that distributed to individuals. Procedures must include periodic media inventories in order to validate the effectiveness of these controls.

Procedures for data retention and disposal must be maintained and must include the following:

- legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data
- provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data
- coverage for all storage of cardholder data, including database servers, mainframes, transfer directories, and bulk data copy directories used to transfer data between servers, and directories used to
- a programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, an audit process, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements
- destruction of media when it is no longer needed for business or legal reasons as follows:
- cross-cut shred, incinerate, or pulp hardcopy materials
- purge, degauss, shred, or otherwise destroy electronic media such that data cannot be reconstructed

Credit card numbers must be masked when displaying cardholder data. Those with a need to see full credit card numbers must request an exception to this policy using the exception process.

Unencrypted Primary Account Numbers may not be sent via email

Procedures for data control must be maintained by each department and must incorporate the following:

- Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities
- Assignment of privileges is based on individual personnel's job classification and function
- Requirement for an authorisation form signed by management that specifies required privileges
- Implementation of an automated access control system

For critical employee-facing technologies (inclusive of remote access technologies, removable electronic media, email usage, internet usage, laptops, and personal data/digital assistants), departmental procedures shall require:

- explicit management approval to use the devices
- that all device use is authenticated with username and password or other authentication item (for example, token)
- a list of all devices and personnel authorised to use the devices
- labelling of devices with owner, contact information, and purpose
- automatic disconnect of remote access technology sessions after a specific period of inactivity
- activation of remote access technologies used by vendors only when needed by vendors, with immediate deactivation after use

Departmental usage standards shall include:

- acceptable uses for the technology
- acceptable network locations for the technology
- a list of company-approved products
- prohibition of the storage of cardholder data onto local hard drives and removable electronic media when accessing such data via remote access technologies
- prohibition of copy, move, storage and print functions during remote access

The ICT Security Manager is responsible for overseeing the ICT Security policy and:

- creating and distributing security policies and procedures
- monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel
- creating and distributing security incident response and escalation procedures that include:
- roles, responsibilities, and communication
- coverage and responses for all critical system components
- notification, at a minimum, of credit card associations and acquirers
- reference or inclusion of incident response procedures from card associations
- analysis of legal requirements for reporting compromises
- annual testing
- plans for periodic training

- a process for evolving the incident response plan according to lessons learned and in response to industry developments
- maintaining a formal security awareness program for all employees that provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)

ICT shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).

System and Application Administrators shall:

- monitor and analyse security alerts and information and distribute to appropriate personnel
- administer user accounts and manage authentication
- monitor and control all access to data
- maintain a list of service providers
- ensure there is a process for engaging service providers including proper due diligence prior to engagement
- maintain a program to verify service providers' PCI-DSS compliant status, with supporting documentation

IT are responsible for tracking employee participation in the security awareness program, including:

- facilitating participation upon appointment
- ensuring that employees acknowledge in writing that they have read and understand the company's information security policy

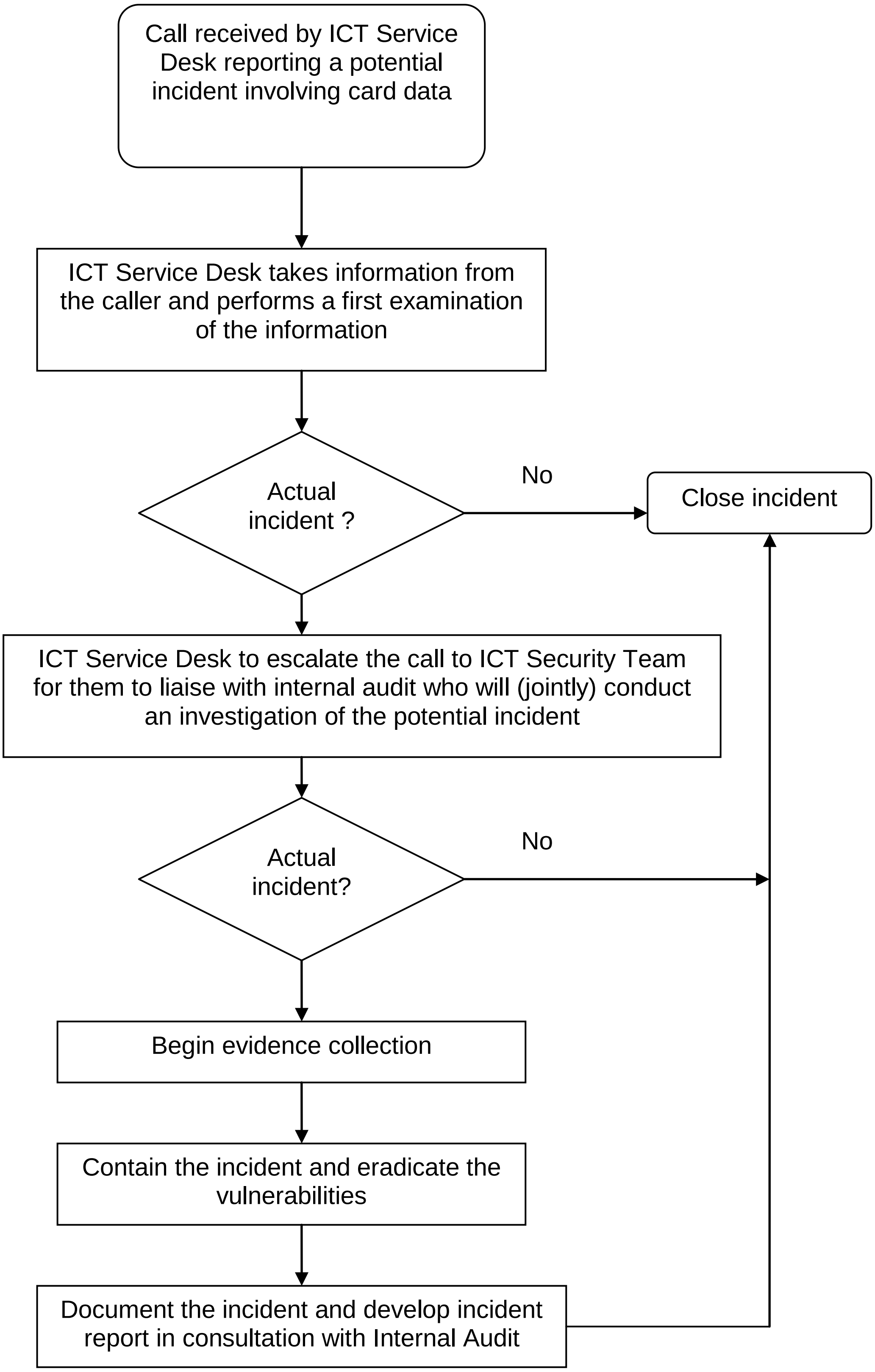
Human Resources are responsible for screening potential employees prior to hire to minimise the risk of attacks from internal sources

Internal Audit is responsible for executing an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.

Head of ICT will ensure that for service providers with whom cardholder information is shared:

- written contracts require adherence to PCI-DSS by the service provider
- written contracts include acknowledgement or responsibility for the security of cardholder data by the service provider

PCI DSS Incident Response Procedure



Call received by ICT Service Desk reporting a potential incident involving card data
ICT Service Desk takes information from the caller and performs a first examination of the information
Actual incident ?
No
Close incident
ICT Service Desk to escalate the call to ICT Security Team for them to liaise with internal audit who will (jointly) conduct an investigation of the potential incident
Actual incident?
No
Begin evidence collection
Contain the incident and eradicate the vulnerabilities
Document the incident and develop incident report in consultation with Internal Audit