PCI DSS Incident Response Plan

I. Introduction

This Incident Response Plan defines what constitutes a security incident specific to the OUHSC cardholder data environment (CDE) and outlines the incident response phases.

For the purpose of this Plan, an incident is an event in which cardholder data in any format -- physical or digital media (**truncated card numbers are not card holder data**) -- has been or is believed to be lost, stolen, or accessed by an individual unauthorized to do so.

This Incident Response Plan is dependent upon the merchant and/or CDE Resource and Data Owners being compliant with the Payment Card Industry Data Security Standard (PCI DSS) and all applicable OUHSC IT Security policies.

This Incident Response Plan will be reviewed and tested annually by the PCI Governance Group to account for changes to\updates in the environment and\or industry trends.

II. Incident Response Roles and Responsibilities

A. Business Unit

The Business Unit must establish policies and\or procedures for card handlers, including back office personnel, and IT administrative staff that address incident reporting both internally and to membership of the PCI Incident Response Team.

In the event of a breach or suspected breach of credit card information, the Business Unit will be responsible for:

- Documentation specific to the incident
- Activities and actions required for escalation
- Notification and response
- Any fines, judgments, and legal fees and expenses associated with the event
- Corrective actions to remediate causes for the breach
- Actions to bring affected systems, environments, and entities into compliance with the PCI DSS
- Reimbursement of costs incurred by other University departments as a result of the incident
- All costs associated with the above

B. Card Handlers and Back Office Personnel

Staff from IT support functions, Business Unit staff, card handlers, and back office personnel are responsible for following the incident discovery, reporting, and response procedures identified in Section III below and as directed by the OUHSC PCI Incident Response Team.

C. IT System Administrators and Tier 1s

IT system administrators and Tier 1s are responsible for following the incident discovery, reporting, and response procedures identified in Section III below, as directed by the OUHSC PCI Incident Response Team, and/or as approved by the PCI Governance Group.

D. Office of the Bursar

The Office of the Bursar will oversee incidents involving payment cardholder data, and will provide notice to the payment card processor, global payment brands, and acquiring banks, as appropriate, according to each entity's respective reporting requirements.

E. Office of Legal Counsel

The Office of Legal Counsel will be responsible for determining any obligation of the University to report a breach to the State of Oklahoma for compliance with the State of Oklahoma Data Breach Laws.

F. The OUHSC PCI Incident Response Team

The OUHSC PCI Incident Response Team will consist of, at a minimum, the HSC Bursar, the Bursar's Merchant Services Representative, the PCI Compliance Officer, and the Director of IT Security Operations (SEC OPS) or an additional member of IT Security Operations.

All PCI related incidents are to be reported to and managed by the OUHSC PCI Incident Response Team. The PCI Response Team will review all incidents to determine if a breach has occurred and will assist the affected department in mitigating future exposure of cardholder data and the associated risks. In addition, the PCI Response Team will make a determination regarding whether OUHSC policies and/or processes need to be revised or created, to avoid a similar incident in the future and whether additional safeguards are required.

G. PCI Governance Group

The PCI Governance Group will determine whether breach notification to the card brands and\or the card holders is required or warranted and will approve and direct any notification and/or reporting required by the responsible departments.

III. Incident Response Phases

A. Incident Discovery

Anytime an employee reasonably believes University customer credit card information may be at risk, the employee should report it in accordance with the established policies and/or procedures of the Business Unit where the potential risk is identified. The following are examples of events or observations that should be reported.

- The loss or theft of any form of media or hardware used as a point of interaction with credit card data. (Thefts should also be reported to the proper law enforcement agency at the time of the incident, and the Merchant and/or Business Unit must maintain a record of the report in accordance with University record retention policies.)
- Any signs of tampering with hardware used as a point of interaction with credit card data.
- Any observed activity outside that of normal operation; for example, a login or credit card transaction activity occurring after normal business hours.
- Virus or malware detection on any system that stores, transmits, processes, or accesses credit card data.
- Any system event or alert indicating a possible compromise or unauthorized access to a system that stores, transmits, processes, or accesses credit card data.
- Any violation of PCI policy or standards

B. Event Assessment

A member of SEC OPS or the Service Desk will open a ticket in ServiceNow to document when the incident is reported, by whom, and what is being reported. The ticket will be assigned to SEC OPS, which will alert both the Director of SEC OPS and the PCI Compliance Officer on the PCI Response Team. The PCI Response Team will also start a PCI Incident Report utilizing the PCI Incident Report Template. No other information related to the incident or its investigation will be included in ServiceNow due to privacy concerns. All documentation related to the incident must be maintained on secure University resources.

A reported incident will be assessed by the PCI Response Team with the reporting Merchant/Business Unit. The PCI Response Team will make a determination regarding whether the event put cardholder data at risk and should be elevated to a possible breach.

An event involving loss or theft of media containing full card numbers (whether encrypted or not) will automatically be elevated to possible breach status.

If the PCI Response Team determines that no cardholder data was put at risk by the reported incident, the PCI Response Team will close the incident, but it may also require the Business Unit or Merchant involved to put corrective measures in place. If the PCI Response Team determines that cardholder data was put at risk by the reported incident, the PCI Response Team will elevate the incident to a possible breach status.

C. Breach Assessment

Once an incident has been elevated, isolation or containment processes for the affected cardholder data environment will be determined and implemented by the Merchant/Business Unit responsible for the resource, and the PCI Response Team will begin a formal investigation.

After the investigation, the PCI Response Team will make a probability of breach determination.

The PCI Governance Group will determine what the University's reporting obligations are and will make a reporting decision regarding notice to the merchant provider, card brands, and/or cardholders.

The PCI Response Team will make a decision as to whether to bring in a PCI Forensics Investigator to perform a complete forensics investigation, and impact determination as defined by the Payment Card Industry Security Standards Council (PCI SSC).

The PCI Response Team, working with the Merchant/Business unit, will identify the potential number of affected card numbers.

D. Reporting

All notices and reports to the State, payment card processor, global payment brands, and acquiring banks; law enforcement and cardholders will be submitted to the PCI Governance Group for review and approval prior to distribution.

1. The Bursar will make any necessary reports to the payment card processor, global payment brands, and acquiring banks, as required by each entity. (See Appendix A.)

2. The Merchant/Business Unit affected will perform any needed internal, law enforcement, and cardholder breach notifications as directed by the PCI Governance Group.

E. Post Breach Determination Activities

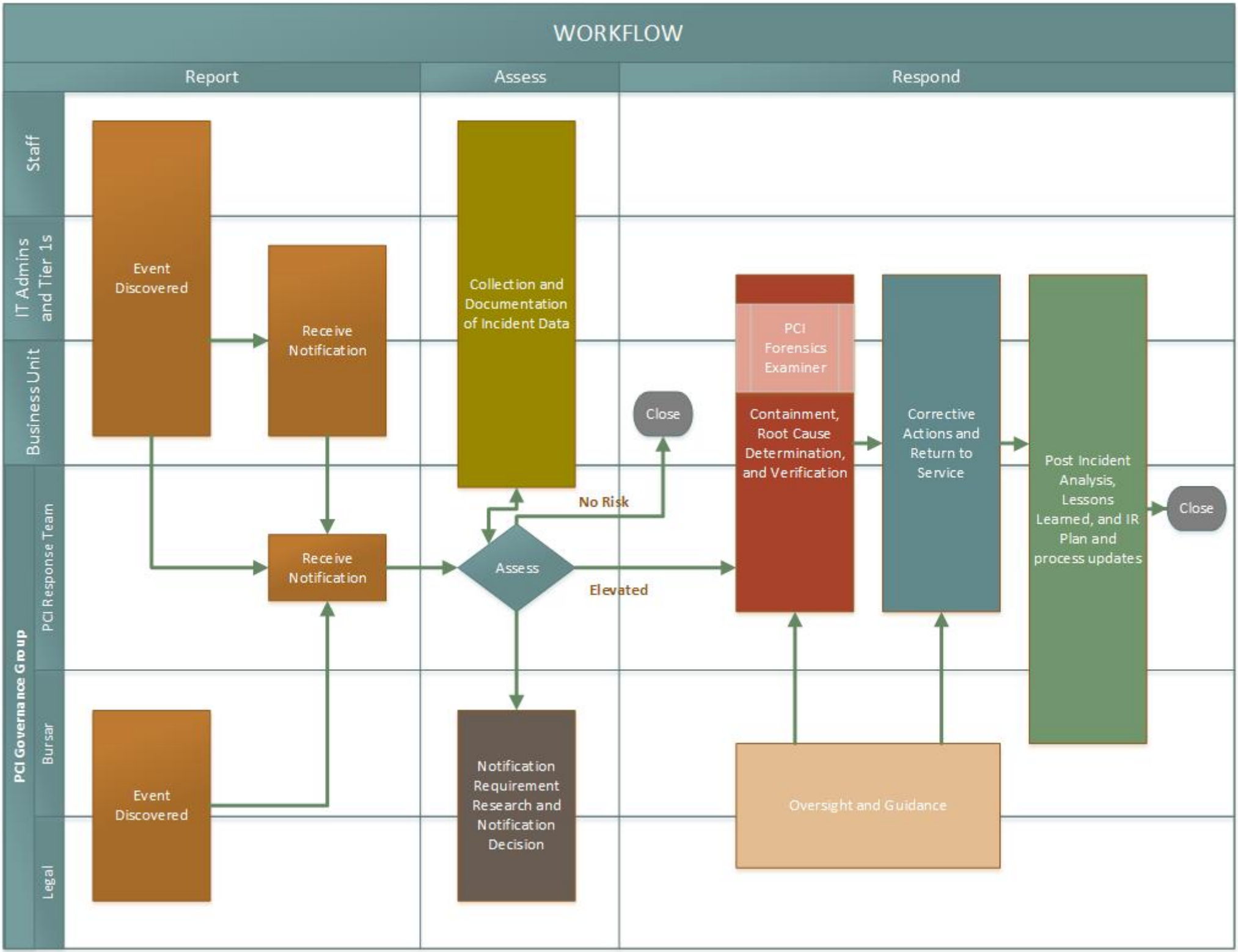
The Merchant/Business Unit affected will perform and document a root cause remediation, with the assistance from PCI Response Team if needed, and present to the PCI Governance Group for approval.

The PCI Response Team will conduct a recovery and compliance verification of the Merchant/Business Unit prior to returning the area's affected resource to service.

The PCI Response Team will conduct a post incident meeting to review the incident and determine what, if any, corrective adjustments to the CDE and related policies and procedures are needed to help prevent a similar event, as well as whether any adjustment to the Incident Response Plan itself is needed.

If adjustments are needed, the PCI Response Team will establish a corrective action plan and assign it to the entity responsible for the area needing adjustment.

The PCI Response Team will document the assessment and resolution in ServiceNow and will close the incident.


WORKFLOW
Report
Assess
Respond
Staff
IT Admins and Tier 1s
Business Unit
PCI Governance Group
PCI Response Team
Bursar
Legal
Event Discovered
Receive Notification
Event Discovered
Receive Notification
Collection and Documentation of Incident Data
Close
No Risk
Assess
Elevated
Notification Requirement Research and Notification Decision
PCI Forensics Examiner
Containment, Root Cause Determination, and Verification
Corrective Actions and Return to Service
Post Incident Analysis, Lessons Learned, and IR Plan and process updates
Close
Oversight and Guidance

Appendix A: Card Brand and Merchant Provider Reporting*

First Data Merchant Services

Complete and submit document: FDMS Potential Data Compromise Incidence Form.doc

VISA USA

Follow VISA document: CISP RESPONDING TO A DATA BREACH.PDF

MasterCard

Follow MasterCard document: MASTERCARD ACCOUNT DATA COMPROMISE USER GUIDE.PDF

Discover Card

Specific Steps:

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102

2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances

3. Prepare a list of all known compromised account numbers

4. Obtain additional specific requirements from Discover Card

*Subject to revision, based on Card Brand and Merchant reporting requirement changes.