**Incident Response Plan (IRP)**

**Purpose**  
This Incident Response Plan (IRP) provides a structured approach to detect, respond to, and mitigate security incidents involving cardholder data (CHD) in compliance with **PCI DSS Requirement 12.10** and related sub-requirements.

**Scope**

This plan applies to all systems, employees, vendors, and contractors involved in the processing, storage, or transmission of CHD.

**1. Roles and Responsibilities**

The **Incident Response Team (IRT)** ensures compliance with PCI DSS **Requirement 12.10.5** by clearly defining roles and responsibilities.

| **Role** | **Responsibility** |
| --- | --- |
| **Incident Response Manager** | Coordinates the response process and ensures compliance with PCI DSS requirements. |
| **Forensic Specialist** | Conducts analysis and preserves evidence in compliance with **Requirement 10.7**. |
| **IT Specialist** | Implements containment, eradication, and recovery strategies as per **Requirement 6.6**. |
| **Compliance Officer** | Ensures actions align with PCI DSS and regulatory requirements (**Requirement 12.1**). |
| **Communications Lead** | Manages internal and external communications to meet **Requirement 12.10.1**. |

**2. Incident Categories**

Incidents are categorized based on their impact on CHD and related systems, aligning with PCI DSS **Requirement 12.10.3**.

| **Category** | **Examples** |
| --- | --- |
| **Low Impact** | Suspicious but non-critical activity (e.g., failed login attempts). |
| **Medium Impact** | Potential CHD exposure (e.g., unauthorized access or vulnerabilities). |
| **High Impact** | Confirmed CHD breach (e.g., malware attacks or critical system compromise). |

**3. Incident Response Procedures**

**Step 1: Identification**

* Use monitoring tools to detect suspicious activity, as per **Requirement 10.6**:
  + SIEM (e.g., Splunk, ELK Stack) for log monitoring.
  + Endpoint detection (e.g., FireEye, CrowdStrike).
  + Web application firewalls (WAF) for real-time threat detection (**Requirement 6.6**).
* Validate incidents by reviewing:
  + Logs (**Requirement 10.5**).
  + User activity patterns.
* Classify the severity based on CHD impact (**Requirement 12.10.3**).

**Step 2: Containment**

* Implement **short-term containment** measures as per **Requirement 12.10.4**:
  + Disconnect affected systems from the network.
  + Disable compromised user accounts (**Requirement 8.1.4**).
* Implement **long-term containment** strategies:
  + Apply patches and updates (**Requirement 6.2**).
  + Strengthen firewall and IDS/IPS configurations (**Requirement 1.2**).

**Step 3: Eradication**

* Eliminate threats while maintaining CHD security (**Requirement 6.5**):
  + Remove malware or unauthorized tools.
  + Update antivirus and endpoint security tools (**Requirement 5.1**).
  + Conduct vulnerability scans to confirm systems are clean (**Requirement 11.2**).

**Step 4: Recovery**

* Restore operations securely (**Requirement 12.10.5**):
  + Rebuild affected systems from validated, secure backups (**Requirement 9.5**).
  + Verify system security and test functionality before reconnecting to production environments (**Requirement 6.6**).
  + Monitor for any recurring issues.

**Step 5: Lessons Learned**

* Conduct a post-incident review within **10 business days**:
  + Document root cause analysis (**Requirement 12.10.7**).
  + Timeline actions and identify preventive measures to reduce future risks.

**4. Incident Reporting**

* Notify stakeholders within **24 hours** of an incident as per **Requirement 12.10.1**.
* Provide incident details to regulatory bodies when required (**Requirement 12.10.2**).
* Maintain a detailed incident log:
  + Date and time of the incident (**Requirement 10.3**).
  + Systems and data affected.
  + Actions taken during response.

**5. Evidence Preservation**

* Preserve the following as per **Requirement 10.7**:
  + Logs (network, system, and application).
  + Forensic images of affected systems.
  + Emails and communications related to the incident.
* Store evidence securely to maintain the chain of custody.

**6. Communication Plan**

* **Internal Communication**:
  + Notify team members and employees via predefined channels (**Requirement 12.10.4**).
* **External Communication**:
  + Only authorized personnel (e.g., Communications Lead) may release information externally.
  + Collaborate with third-party forensic or legal teams if required (**Requirement 12.9**).

**7. Training and Testing**

* Conduct annual training for all employees handling CHD as per **Requirement 12.6**.
* Test the IRP through tabletop exercises or simulated breach scenarios at least once per year (**Requirement 12.10.2**).

**8. Policy Review**

* The IRP must be reviewed and updated:
  + Annually (**Requirement 12.11**).
  + After significant changes to systems or business processes.
  + Following a security incident (**Requirement 12.10.5**).

**Approval**

This plan is approved by:  
**Name:** Mohamed Hamza  
**Title:** Senior Incident Response analyst  
**Date:** 1/24/2025