Flow Chart for Suspected Breach

**SUSPICIOUS ACTIVITY REPORTED**

**BREACH SUSPECTED**

- Do NOT turn off the PC/server
- Disconnect PC/server from network
- Document (via Incident Response Form)
  - Suspicious activity
  - Steps taken to date
  - Personnel involved

**Notify Accountant and IT Sr. Systems Manager**

**Incident Response Team**

- Verify/Investigate breach
  - Ensure system(s) are isolated
  - Gather/log central evidence (firewalls, file integrity, IDS, AV, etc.)
  - Analyze local machines/logs
  - Forensic analysis on breached PC
- Prepare INITIAL incident report (via Incident Response Form) and consult with
  - Public Relations
  - Acquiring Bank and Card Brands

- Issue FINAL incident report
- Prioritize/complete any remediation items
Northeast Ohio Medical University – Incident Response Form & Guidelines

Report Date/Time: ________________________________

Confidentiality

Distribution of this document is limited to the NEOMED Accounting Department. Access should only be granted to those with a business related need-to-know. If you have any questions pertaining to the distribution of this document, please contact the Controller.

Reporting Party

Name: ________________________________
Title: ________________________________
Telephone/Email: ________________________________

Summary

The summary is at a high level, suitable for upper management. Elements include:

- Basic description of the incident
- Systems, services and/or user communities impacted by the incident
- Whether service was not impacted, degraded, or interrupted
- Duration of the incident (start to finish)

Details of the Incident, Steps Taken To-Date

Specifically, what caused the incident (who, what, where, when, how) and what steps have been taken by the reporting party to-date.

- Details of the incident
- Detail the flow of the incident response (i.e., John -> Jim -> Mike)

Steps Taken To-Date:

<table>
<thead>
<tr>
<th>Steps Taken To-Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network cable unplugged (time/date):</td>
</tr>
<tr>
<td>Last time machine rebooted (time/date):</td>
</tr>
<tr>
<td>When anomalous activity was noticed (time/date):</td>
</tr>
<tr>
<td>Incident Response Team notified (time/date):</td>
</tr>
<tr>
<td>Additional Details:</td>
</tr>
</tbody>
</table>

Name: ________________________________
Title: ________________________________

Please use additional blank pages as necessary.
Incident Response Team Lead

Identify the Incident Response team member assigned to take the lead on this incident

Name: ____________________________  Title: ____________________________  Telephone/Email: ____________________________

Incident Analysis

Identify the Incident Response

PCI Event Yes/No: ____________________________  Justification: ____________________________

If PCI Event is “Yes,” complete the following steps

Time/date of Step E, Internal Notification

PCI IRP Step E, Internal Notification: ____________________________

Steps taken during forensic investigation

ATTACHMENTS

Please attach any supporting documents. These documents may include:

- Logs or error messages
- Contents of trouble tickets
- Contents of e-mail

Conclusion, Findings and Recommendations

- What was the basic cause of the incident?
- What could have prevented this?
- Impact (none, degraded performance, downtime)
- Business criticality (revenue producing, business critical, low)
  estimated cost (impact + business criticality)
- What would prevent the incident from reoccurring?
- What additional actions or research need to take place?

Name: ____________________________  Title: ____________________________

Please use additional blank pages as necessary.