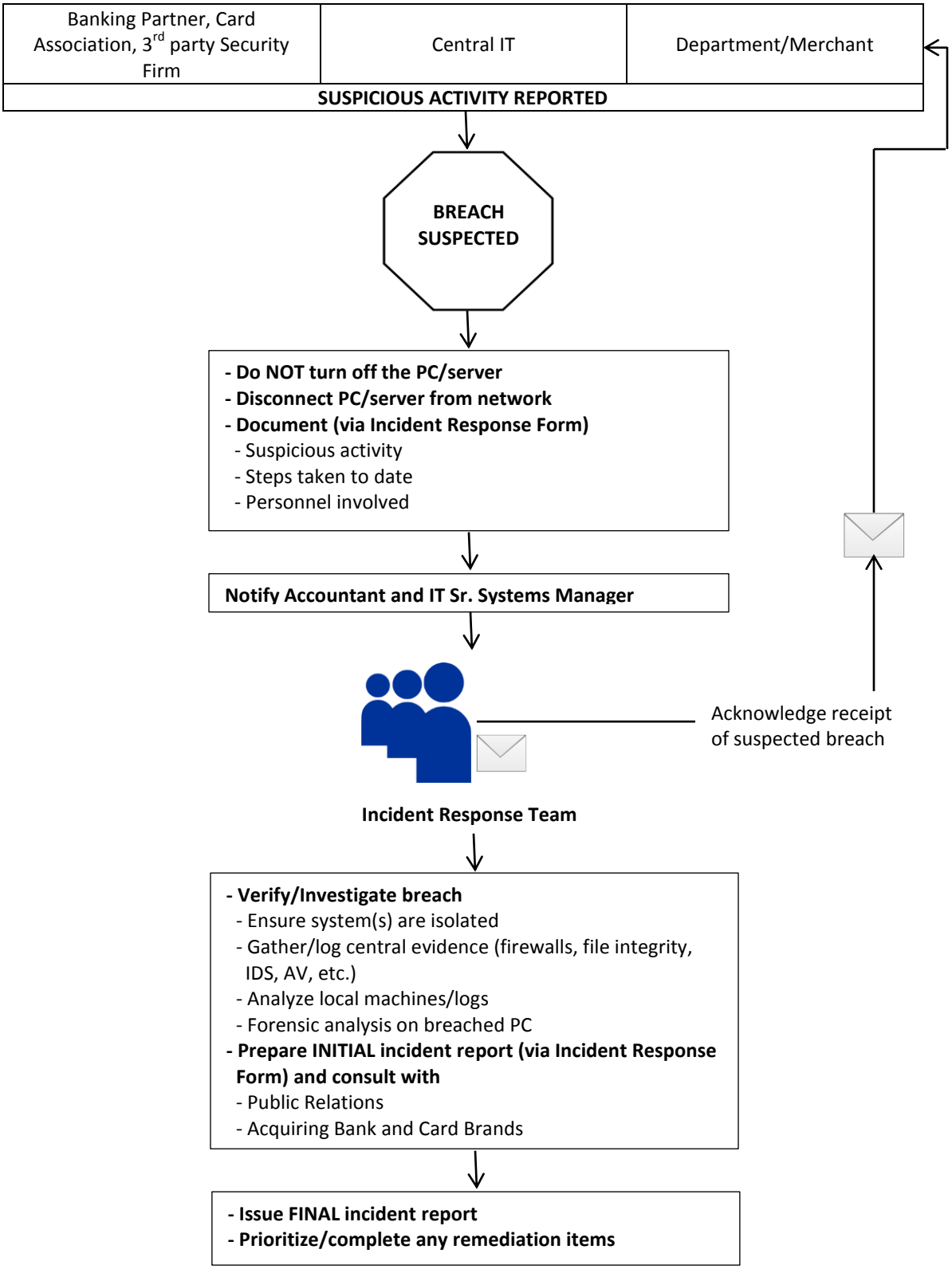
Flow Chart for Suspected Breach



Northeast Ohio
MEDICAL UNIVERSITY

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:	
Network cable unplugged (time/date):	
Last time machine rebooted (time/date):	
When anomalous activity was noticed (time/date):	
Incident Response Team notified (time/date):	
Additional Details:	

_____ _____

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.