Security Incident Response Report Form

I. Incident Identification Information

A. Date/Time of Notification: ____

B. Incident Detector's Information:

Name: ____

Title: ____

Phone: ____

Email: ____

C. Date/Time Detected: ____

D. Location: ____

E. System or Application: ____

____

____

II. Incident Summary

A. Type of Incident Detected: ____

____

____

____

____

____

B. Description of Incident: ____

____

____

____

____

____

C. Names and Contact Information of Others Involved: _______________________________

____

____

____

III. Incident Notification

A. Incident Response Team Member first notified ___________________________________

B. IT or IS Director ____

C. Information Owner ____

D. System or Application Vendor____

E. Human Resources ____

F. Legal ____

G. University Communications ____

IV. Incident Response Actions

A. Identification Measures (Incident verified, Assessed, Options Evaluated): _____________

____

____

____

B. Containment Measures: ____

____

____

____

C. Evidence Collected (System logs, etc.): ____

____

____

____

D. Eradication Measures: ____

____

____

____

E. Recovery Measures: ____

____

____

____

F. Other Mitigation Actions: ____

____

____

____

V. Incident Response Evaluation

A. How well did work force members respond? ______________________________________

____

____

____

B. Were the documented procedures followed? Were they adequate? _________________

____

____

____

C. What information was needed sooner? ____

____

____

____

D. Were any steps or actions taken that might have inhibited the recovery? ____________

____

____

____

E. What could work force members do differently next time an incident occurs? ________

____

____

____

F. What corrective actions could prevent similar incidents in the future? _______________

____

____

____

G. What additional resources needed to detect, analyze and mitigate future incidents? ___

____

____

____

H. Other conclusions or recommendations? _______________________________________

____

____

____

VI. Incident Follow Up

A. Recommended actions carried out: ____

____

____

____

B. Initial report completed by: ____

____

C. Follow up completed by: ____

____

VII. QA/QC Review of Incident & Report Form

A. Incident Response Team Member ____

B. IT or IS Director ____

C. Senior Management ____

D. Other ____