**ADMINISTRATIVE PRACTICE LETTER**

**SUBJECT: Information Security Incident Response**

***APPENDIX B. Security Incident Report***

# Security Incident Report

## Contact *Information*

Name: _____ Title: _____

Email: _____ Telephone: _____

Department: _____ Date Report Submitted: _____

## Incident Information

Physical Location(s) of affected computer system/network (be specific):

_____

Date/Time of incident: _____ Duration of incident: _____

Is affected system/network critical to department's mission?

### How was *the* incident discovered?

☐ System Logs ☐ Performance Degradation ☐ Third Party

☐ Notified by user ☐ Other

### Type of Incident:

☐ Unauthorized Access ☐ Network Attacks/Disruption ☐ Malware

☐ Theft or Loss ☐ Physical Intrusion/Break-in ☐ Social Engineering

☐ Policy Violation ☐ Other _____

What computer/Operating Systems were affected?

_____

The apparent source (IP address) of the intrusion/attack: _____

# ADMINISTRATIVE PRACTICE LETTER

## SUBJECT: Information Security Incident Response

Incident Data Classification:

☐ Security Incident involving Compliant Data ☐ Security Incident involving Business Sensitive Data

☐ Security Incident involving Unclassified Data

What actions and technical mitigation have been taken?

Additional Remarks: