LSU Incident Response Data Template

Incident Category (see http://www.us-cert.gov/federal/reportingRequirements.html; CAT 0-CAT 6):

Brief Description:

Discovery Data
Date and Time of Discovery:
Discovered by (person / organization):
Discovery Method (e.g. Help Desk, NetEnforcer, proactive scan, etc): 

System(s) Ownership Data
Responsible Network Contact:
Responsible Organization (e.g. College of Business, ITS, etc.):

System(s) Technical Data
System(s) Physical Location:
System(s) Host Name:
System(s) IP Address(es):
System(s) Operating System and Version (e.g. Windows XP Professional with Service Pack 2):
System(s) Workloads (e.g. office worker’s desktop, file server, web server, etc.):
System(s) Security Realm State (e.g. joined to Active Directory, joined to campus NT 4.0 domain, standalone, etc):
System(s) Security Update State (on Windows systems, paste or attach results of Microsoft Baseline Security Analyzer scan; on other systems, use results of applicable package management tool):

Vulnerability and Forensic Data
System(s) Network Attack Surface (paste or attach results of Retina or Nessus scan)

System(s) Process List (paste or attach output of process list from time of discovery; on Windows, run ‘tasklist /svc /v’; on Unix based systems run ‘ps –A’)

System(s) Network Connections (paste or attach output of netstat; on both Windows and Unix based systems, run ‘netstat –a’)

**Personally Identifiable Information**

Is Personally Identifiable Information (PII) Stored or Processed on the System:

What Types of PII are Stored or Processed (e.g. SSNs, Credit Cards, etc.):

Approximately How Many Parties’ PII are Stored or Processed (e.g. 1000 students):