University of New Hampshire[1]
Technology Incident Report

Contact Information (Organization where the incident took place)

Department Name:	**Computer Name:**	
IT Specialist or Investigator Name:	**Phone #:**	**Email address:**

Incident Information

Date incident *occurred*:	**Date incident *discovered*:**	**# Machines, persons or records affected:**
Time incident *occurred*:	**Time incident *discovered*:**	

Type of Incident:
System Compromise/Intrusion
☐ External ☐ Internal Other _____
Loss, Theft, or Missing
☐ Computer ☐ Data ☐ Media ☐ Other
Malicious Code
☐ Trojan ☐ Virus ☐ Worm ☐ Other _____
☐ Web Site Defacement
☐ Denial of Service
☐ Infrastructure Damage
☐ Unauthorized connection
☐ Information Compromise

Extent of Success:
☐ Reconnaissance
☐ Intrusion Attempt
☐ Confirmed Intrusion
☐ Confirmed Data Loss
☐ Confirmed Damage
Other _____

Security Category (According to data classification): ☐ Low (Public Data): *limited* adverse affect ☐ Moderate (Sensitive Data): *serious* adverse affect ☐ High (Restricted Data): *severe or catastrophic* adverse affect Combination of Above: _____	**Information Type or Data Class Breached/Damaged:** ☐ Legally Protected Data ☐ Data Protected by Contract, Policy or Directive ☐ Public Data ☐ Other _____	**Which critical infrastructure was affected, if any?**

MAC address of affected machine(s):	**Domain name of affected machine(s):**
Operating system(s) of affected machine(s):	**Last time the affected machine(s) patched**:
Functions of affected machine(s):	**Application software affected:**

Description of incident:

Method of detection:

What security infrastructure was in place:

Attacker information:

IP address(es) of attackers:	**Destination Port(s) and Protocol(s):**
Domain name(s) of attacker(s):	**Country(ies) of attacker(s):** **Asia/Pacific, Europe**

Suspected method of intrusion/attack:

Suspected perpetrators and/or possible motivations:

Name of Trojan(s) or malicious code(s) (if applicable):	**Evidence of spoofing:**

[1] Adapted for use at UNH with permission from UNH Department of Residential Life

Impact and Actions Taken

Assessment of the impact of the incident:

Did the intrusion damage any machine(s): **If yes, please describe**:

☐ Yes ☐ No

What actions have been taken:

Who Has Been Notified

☐ Supervisor

☐ CIS IT Security or CIO

☐ USNH Legal Counsel

☐ NH Attorney General

☐ UNH Police

☐ Other _____

If restricted data is involved, have affected people been notified?

Additional Actions That Will Be Taken

Actions that will be taken:

Do you have needed skills and resources?

☐ Yes ☐ No

If no, what do you need?

Debriefing

Who will be included in the debriefing?

☐ Department personnel and leadership

☐ CIS IT Security

☐ USNH Legal Counsel

☐ UNH Police

☐ Supervisor _____

☐ Other _____

When and where will the debriefing take place?

Who will follow up on the debriefing to ensure that any remaining actions items receive appropriate attention?

Where will this report be filed?