

## SENSITIVE DATA EXPOSURE INCIDENT CHECKLIST

INCIDENT # \_\_\_\_\_

Date became aware: \_\_\_\_\_

Date reported to ISO: \_\_\_\_\_

Date affected individuals notified: \_\_\_\_\_

*(should be within one week of incident discovery)*

**Type and scope of data exposed:**

**Incident Team:**

### **STEP 1: IDENTIFICATION**

***Verify that an incident has actually occurred. This activity typically involves the end user, but may also result from proactive incident detection work of Technology Advancement and Support. If it is determined that an incident has occurred, inform the Chief Information Security Officer, and the Support Center.***

Done	Task	Owner	Notes
	<p>1.1 Immediately contain and limit exposure:</p> <ul style="list-style-type: none"> <li>- If electronic device has been compromised:               <ul style="list-style-type: none"> <li>o Disable network connection (NOT power cable) from the compromised device</li> <li>o Do <u>not</u> access (do not logon) or alter compromised device</li> <li>o Do <u>not</u> power off the compromised device</li> </ul> </li> <li>- Write down how the incident was detected and what actions have been taken so far. Provide as much specificity as possible, including dates, times, and impacted machines, applications, websites, etc.</li> </ul> <p>RESOURCES:</p> <ul style="list-style-type: none"> <li>a) IT Incident Response Overview</li> <li>b) Northland' Incident and Risk Assessment Policy</li> </ul>	End user or technician	

**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	<p>c) EDUCAUSE Information Security Incident Management <a href="https://spaces.internet2.edu/display/2014infosecurityguide/Information+Security+Incident+Management">https://spaces.internet2.edu/display/2014infosecurityguide/Information+Security+Incident+Management</a></p>		
	<p>1.2 Technology Advancement and Support immediately:</p> <p><i>a) Calls the Support Center at (928) 524-7447.</i> <i>b) Notifies the Information Security Group (ISG) (928) at 532-6769 or email infosec@NPC.edu</i> <i>c) Reports incident according to the NPC Incident Response Overview.</i></p> <p><i>RESOURCES:</i> <i>a) TAS Incident Response Overview</i> <i>b) Information Security Incident Response Form (long or short)</i></p>	TAS / ISG	
	<p>1.3 If the incident involves electronic devices or media stolen or lost within the local community, also alert law enforcement.</p> <p><i>a) Notify Campus Security</i></p>	ISG	
	<p>1.4 Conduct preliminary assessment of type and scope of data exposed. If the incident potentially exposed sensitive data, notify all appropriate institution officials and keep them informed as incident investigation progresses:</p>	ISG	

**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	<p><i>EXAMPLES:</i></p> <ul style="list-style-type: none"> <li>a) CTO</li> <li>b) CFO</li> <li>c) CHRO</li> <li>d) Campus President (or his/her Chief of Staff)</li> <li>e) Counsel for the College</li> <li>f) Law enforcement, e.g., campus security, FBI local office, Secret Service local office</li> <li>g) Public Affairs</li> <li>h) Appropriate Data Steward(s) for the type of data potentially at risk</li> <li>i) Finance office, if credit card #, bank account #, or other sensitive financial data potentially at risk</li> </ul>		
1.5	<p>If there is evidence of criminal activity connected with the incident determine interest of law enforcement in leading the investigation. If law enforcement (e.g., FBI) takes lead, subsequent steps may be performed by law enforcement or require authorization from the law enforcement lead.</p>	ISG	
<p><b>STEP 2: DAMAGE CONTAINMENT AND DATA EXPOSURE ASSESSMENT</b>  <b>Identify an Incident Response Lead and assemble an incident response team charged with limiting further damage from the incident. Conduct a thorough assessment of the type and scope of data exposed following applicable laws, regulation and policy.</b></p>			
2.1	<p>Assemble Incident Response Team – Information Security Group (ISG) will lead this effort.</p> <p><i>GUIDANCE: Ensure that the representative from the organizational unit where the incident occurred participates and that this individual is high enough in the organization to make necessary decisions.</i></p>	ISG/Incident Response Team	

**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	<p>2.2 Review incident response process and responsibilities with Incident Response Team</p> <ul style="list-style-type: none"> <li>- Provide each member with current IT Incident Checklist</li> <li>- Discuss communications strategy</li> <li>- Stress importance of maintaining chain of custody</li> </ul> <p><i>GUIDANCE: Discussing the rules of communication with the team at this stage is particularly important to ensure accuracy of facts among team members and between the team and appropriate University officials.</i></p> <p><i>EXAMPLES:</i></p> <ul style="list-style-type: none"> <li>a) Team members must not discuss the incident with anyone outside the team until and only if authorized to do so by the Chief Information Officer or President.</li> <li>b) All documentation created by team members must be fact-based, as it may become important reference or evidence</li> <li>c) Daily conference call of team members will be held discuss status.</li> <li>d) Instruct team to track time spent on the incident.</li> </ul>	ISG/Incident Response Team	
	<p>2.3 Collect and preserve evidence</p> <p><i>GUIDANCE:</i> <i>Collect physical and cyber evidence that provides a clear, detailed description of how the sensitive data was compromised.</i></p> <p><i>EXAMPLES:</i></p> <ul style="list-style-type: none"> <li>a) Image of hard drive(s)Physical equipment</li> <li>b) Network traffic flow to/from compromised device</li> <li>c) Workstation and application logs</li> <li>d) Access logs</li> <li>e) Digital photographs of the evidence and surrounding area</li> </ul> <p><i>RESOURCES:</i> <a href="http://www.educause.edu/Resources/ForensicOverview/161135">http://www.educause.edu/Resources/ForensicOverview/161135</a> <a href="http://www.cybercrime.gov/ssmanual/index.html">http://www.cybercrime.gov/ssmanual/index.html</a></p>	ISG/Incident Response Team	

**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	<p><a href="http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf">http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf</a></p>		
	<p>2.4 Establish and maintain appropriate chain of custody for all evidence.</p> <p><i>GUIDANCE:</i> <i>Inventory pieces of evidence and track who accessed, used, stored, moved or returned each piece of evidence and when it was accessed.</i></p> <p><i>EXAMPLES:</i></p> <ul style="list-style-type: none"> <li>a) Establish what exactly the evidence is</li> <li>b) Document who handled it and why</li> <li>c) Document where and how it was stored</li> <li>d) When equipment is moved, ensure that a detailed receipt is signed and dated by the previous person with possession, the mover and the new person with responsibility for the equipment</li> </ul> <p><i>RESOURCES:</i>  <a href="http://www.cert.org/csirts/services.html">http://www.cert.org/csirts/services.html</a>  <a href="http://www.sans.org/score/incidentforms/ChainOfCustody.pdf">http://www.sans.org/score/incidentforms/ChainOfCustody.pdf</a></p>	<p>ISG/Incident Response Team</p>	
	<p>2.5 Take actions needed to limit the scope and magnitude of the incident</p> <p><i>EXAMPLES:</i></p> <ul style="list-style-type: none"> <li>a) <i>If the incident involves sensitive data improperly posted on one or more publicly accessible websites, remove active and cached content and request takedown of cached web page(s) indexed by search engine companies and other Internet archive entities</i></li> <li>b) <i>Change passwords that may have been compromised</i></li> <li>c) <i>Cease operation of a compromised application or server</i></li> </ul>	<p>ISG/Incident Response Team</p>	

**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	<p>2.6 Perform forensics and document findings:</p> <ul style="list-style-type: none"> <li>a. Analyze evidence</li> <li>b. Reconstruct incident</li> <li>c. Provide detailed documentation</li> </ul> <p><i>GUIDANCE: Preserve original evidence and work on a copy of data Obtain and preserve with minimal disturbance to units, systems and original evidence Results should be repeatable</i></p>	ISG/Incident Response Team	
	<p>2.7 Complete final assessment and documentation of type and scope of data exposed, as well as the availability and type of contact data for individuals affected</p>	ISG/Incident Response Team	
<p><b>STEP 3: ERADICATION AND RECOVERY</b> <b><i>Take steps to remove the cause of the exposure, reduce the impact of the exposure of the sensitive data, restore operations if the incident compromised or otherwise put out of service a system or network, and ensure that future risk of exposure is mitigated</i></b></p>			
	<p>3.1 Revisit 2.4 and look for additional ways to limit exposure</p> <p><i>EXAMPLES:</i></p> <ul style="list-style-type: none"> <li>a) <i>Run web queries periodically to ensure that the data has not been further exposed or cached.</i></li> <li>b) <i>Review the inventory of equipment and systems impacted and change additional passwords that may have been compromised</i></li> <li>c) <i>Cease operation of a compromised application or server and develop work-arounds</i></li> </ul>	ISG/Incident Response Team	
	<p>3.2 Eradicate and/or mitigate system vulnerabilities, review access privileges and remediate risks to sensitive data stores</p> <p><i>EXAMPLES:</i></p> <ul style="list-style-type: none"> <li>a) <i>Run vulnerability scans on impacted systems;</i></li> <li>b) <i>Review and determine where data resides and make adjustments to ensure increased protection as needed.</i></li> </ul>	ISG/Incident Response Team	

**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	<p>c) <i>Limit access to systems to only those who need it;</i> d) <i>Use software tools to find, delete and secure sensitive data, e.g., Identity Finder</i></p>		
	<p>3.3 Return evidentiary equipment and systems to service once they are secured.</p>		
<p><b>STEP 4: NOTIFICATION</b> <i>Determine the need to give notice to individuals whose data may have been exposed by the incident. Swiftmess in notifying those affected by a breach of personally identifiable information, as well as informing certain government entities, is legally mandated in many states and, depending on the nature of the data, also federal law. Speed is also important from a public relations standpoint. To this end, many of the sub-steps can and should be undertaken in parallel to accommodate these needs.</i></p>			
	<p>4.1 Make decisions based upon Incident Response Team findings</p> <ul style="list-style-type: none"> <li>- Does level of exposure risk warrant notification letters?</li> <li>- If yes, <ul style="list-style-type: none"> <li>• If applicable, has law enforcement authorized notification to affected parties?</li> <li>• Who will issue letter?</li> <li>• Who will handle telephone and email responses to questions from affected individuals? Does expected volume warrant setting up call center?</li> <li>• Does magnitude of exposure warrant a press release? Incident information website?</li> <li>• Does exposure risk warrant free credit monitoring?</li> </ul> </li> <li>- <b><u>If a reasonable risk of exposure does not exist, all remaining sub-steps in this section should be bypassed and STEP 5 Follow-up should commence.</u></b></li> </ul> <p><b>GUIDANCE:</b></p> <p>a) <i>Those responsible for making these decisions will vary from institution to institution, but typically is a subset of officials informed in Sub-step 1.4. Decisions made should be in line with previous decisions or any deviations fully justified. Obviously, all incident notification laws, regulations, and contractual requirements must be followed.</i></p> <p>b) <i>While breach notification laws, regulations, and contractual requirements vary, alternatives to issuing written notices by postal mail are often allowable depending upon the cost of providing notice, the number of individuals who must be notified, and/or the availability of contact information.</i></p>	<p>Appropriate College officials</p>	

**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	<p><i>These alternatives might, for example, include, but are not limited to, one or more of the following: conspicuous posting of notices on the institution’s website, press releases, email notices where addresses are known, telephone notices.</i></p> <p>c) See EDUCAUSE Data Incident Notification Toolkit for further guidance. <a href="https://spaces.internet2.edu/display/2014infosecurityguide/Data+Incident+Notification+Toolkit">https://spaces.internet2.edu/display/2014infosecurityguide/Data+Incident+Notification+Toolkit</a></p>		
	<p>4.2 Collect name and contact information on affected individuals</p> <p><i>GUIDANCE: This could be a laborious process if individuals are not current students, faculty, staff, donors, patients, etc. of the institution. It is advisable that the best sources of address data for former students, faculty, and staff, as well as alumni, volunteers, contractors, and other affiliates of the institutions whose sensitive data are maintained by the institutions be identified in advance, so that notifications can be made quickly in the event of data exposures.</i></p> <p><i>Ensure that data is collected, transmitted and stored securely and removed when it is no longer needed.</i></p>	ISG/Incident Response Team	
	<p>4.3 Set up telephone and email support for affected individual questions:</p> <ul style="list-style-type: none"> <li>- Identify appropriate person(s) to handle calls and emails</li> <li>- Establish telephone call line/routing infrastructure, if not available</li> <li>- Identify/set up telephone number to use</li> <li>- Identify/set up email address to use</li> <li>- Train individuals handling calls and emails, including providing them with a list of anticipated questions and answers</li> </ul> <p><i>GUIDANCE: See EDUCAUSE Data Incident Notification Toolkit – FAQ Section <a href="https://spaces.internet2.edu/display/2014infosecurityguide/Data+Incident+Notification+Toolkit">https://spaces.internet2.edu/display/2014infosecurityguide/Data+Incident+Notification+Toolkit</a> for advice and sample content for telephone and email responder FAQs.</i></p>	ISG/Incident Response Team	
	<p>4.4 If deemed appropriate by institution officials in Sub-step 4.1, create website for affected individuals</p> <ul style="list-style-type: none"> <li>- Identify URL and location</li> <li>- Restrict access until ready to go live</li> </ul>	ISG/Incident Response Team	



**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	<p>- Draft content</p> <p><b>GUIDANCE:</b></p> <p>a) <i>Incident websites are typically reserved for situations in which contact information for individuals affected by the breach is unknown or incomplete.</i></p> <p>b) <i>See EDUCAUSE Data Incident Notification Toolkit – Website Section <a href="https://spaces.internet2.edu/display/2014infosecurityguide/Data+Incident+Notification+Toolkit">https://spaces.internet2.edu/display/2014infosecurityguide/Data+Incident+Notification+Toolkit</a> for advice and sample content</i></p> <p>c) <i>Website content should be approved by appropriate institution officials, e.g.,</i></p> <ul style="list-style-type: none"> <li>• <i>CIO</i></li> <li>• <i>Executive in charge of organization in which incident occurred</i></li> <li>• <i>Office of Institutional Advancement</i></li> <li>• <i>Counsel for the institution</i></li> </ul>		
	<p>4.5 If deemed appropriate by institution officials in Sub-step 4.1, obtain free credit monitoring services for affected individuals</p> <p><b>GUIDANCE:</b> <i>Obtain clear instructions to provide affected individuals signing up for free credit monitoring services and include this information in notification letters, websites, and email/telephone support FAQs.</i></p>	CFO and CIO	
	<p>4.6 If deemed appropriate by institution officials in Sub-step 4.1, prepare press release</p> <ul style="list-style-type: none"> <li>- Identify contact for media</li> <li>- Compose text for press release</li> <li>- Develop talking points</li> </ul> <p><b>GUIDANCE:</b></p> <p>a) <i>Press releases are often reserved for situations in which contact information for individuals affected by the breach is unknown or incomplete, but it's wise to have a pre-approved media statement in hand to use in addressing media inquiries.</i></p> <p>b) <i>See EDUCAUSE Data Incident Notification Toolkit – Press Release Section <a href="https://spaces.internet2.edu/display/2014infosecurityguide/Data+Incident+Notification+Toolkit">https://spaces.internet2.edu/display/2014infosecurityguide/Data+Incident+Notification+Toolkit</a> for advice and sample content.</i></p>	Office of Institutional Advancement	

**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	<p>c) <i>Content should be approved by appropriate institution officials, e.g.,</i></p> <ul style="list-style-type: none"> <li>• <i>Executive in charge of IT for the institution, e.g., Vice President &amp; CIO</i></li> <li>• <i>Executive in charge of organization in which incident occurred</i></li> <li>• <i>Public affairs office</i></li> <li>• <i>Counsel for the institution</i></li> </ul>		
	<p>4.7 Prepare notification letter to affected individuals</p> <ul style="list-style-type: none"> <li>- Identify letter issuer and letterhead to be used</li> <li>- Compose draft text</li> </ul> <p><i>GUIDANCE:</i></p> <p>a) <i>See EDUCAUSE Data Incident Notification Toolkit – Letter Section <a href="https://spaces.internet2.edu/display/2014infosecurityguide/Data+Incident+Notification+Toolkit">https://spaces.internet2.edu/display/2014infosecurityguide/Data+Incident+Notification+Toolkit</a> for advice and sample content.</i></p> <p>b) <i>Letter content should be approved by appropriate institution officials, e.g.,</i></p> <ul style="list-style-type: none"> <li>• <i>CTO</i></li> <li>• <i>Executive in charge of organization in which incident occurred</i></li> <li>• <i>Office of Institutional Advancement</i></li> <li>• <i>Counsel for the institution</i></li> </ul>	<p>Office of Institutional Advancement and TAS</p>	
	<p>4.8 Prepare mailing of notification letters (postage, addresses)</p> <ul style="list-style-type: none"> <li>- Finalize address information</li> <li>- Arrange for mail merge and printing/stuffing` of letter and envelopes</li> </ul> <p><i>GUIDANCE: Avoid personalizing each letter with the affected individuals name, as this increases the risk of mismatched letters and envelopes</i></p>	<p>Office of Institutional Advancement</p>	
	<p>4.9 If required by state law, notify the State’s Attorney General within the required notification timeframe</p>	<p>President / CIO</p>	

**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	<p>4.10 Notify appropriate Federal agency as required by law</p> <p><i>EXAMPLES:</i></p> <p>a) U.S. Department of Education when FERPA-protected student data is exposed</p> <p>b) U.S. Department of Health and Human Services when HIPAA-protected medical data is exposed</p> <p><i>RESOURCES:</i></p> <p>HIPAA: <a href="http://www.hhs.gov/ocr/privacy/">http://www.hhs.gov/ocr/privacy/</a>  <a href="http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html">http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html</a></p> <p>FERPA: <a href="http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html">http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html</a></p> <p>Other data protection laws, <a href="http://protect.iu.edu/cybersecurity/data/laws">http://protect.iu.edu/cybersecurity/data/laws</a></p>	<p>President / CIO</p>	
	<p>4.11 Notify granting organizations and research partners if research data compromised, as dictated by contractual obligations</p>	<p>President / CIO</p>	
	<p>4.12 Notify appropriate third-party service providers for the institution if doing so would reduce the risk of identity theft for affected individuals or dictated by contracts.</p> <p><i>EXAMPLES:</i></p> <p>a) Employee benefit vendors</p> <p>b) Student services vendors</p>	<p>President / CIO/ designated department heads</p>	
	<p>4.13 If Credit Card data exposed, notify the credit card processor(s) or merchant banks</p> <p><i>GUIDANCE: Specific notification requirements are governed by the card brand.</i></p> <p><i>EXAMPLE:</i></p> <p>VISA -- <a href="http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html">http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html</a></p> <p>-</p>	<p>CFO</p>	

**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	4.14 Notify Credit Bureaus as required by State and upon consultation with University Council	CFO	
	4.15 Coordinate simultaneous mailing of letters to affected individuals, issuance of press release if applicable, activation of website if applicable, notifications to regulatory entities and third-party vendors.	Student Services / Office of Institutional Advancement	
	4.16 Ensure that notification of the data breach is added to the record of access to the affected individuals file as required by Federal or State law.	Registrar	
<p><b>STEP 5: FOLLOW-UP</b> <i>Identity lessons learned from the incident, implement any remediation needs, and securely store a complete record of the incident.</i></p>			
	5.1 Collect staff time spent during event and record in the incident documentation (especially for those cases that might be prosecuted)	Unit gathers data from all affected parties and provides to ISG	
	5.2 Schedule a debriefing meeting two to six weeks afterwards to review what could have been done better in responding to the incident.	President, ISG, Office of Institutional Advancement, and appropriate others	
	5.3 Assess remediation needs <ul style="list-style-type: none"> <li>- Issue report to unit manager and executive management if appropriate</li> <li>- Follow up to ensure completed</li> </ul>	ISG	

**Northland Pioneer College  
Sensitive Data Exposure  
Incident Checklist**

	<p><i>EXAMPLES:</i></p> <ul style="list-style-type: none"> <li><i>a) Why was the data stored in a vulnerable place?</i></li> <li><i>b) What more could have been done to avoid the intrusion?</i></li> <li><i>c) Is the unit taking appropriate steps to remediate?</i></li> </ul>		
	<p>5.4 Initiate plans and projects to implement remediation needs.</p> <ul style="list-style-type: none"> <li>- Apply lessons learned and recommended changes to access, sensitive data stores, systems and processes to increase protection</li> </ul>	ISG / Office of Institutional Advancement	
	<p>5.5 Securely file all records, communications, notes, and other incident artifacts. Retain and eventually securely destroy this incident information in accordance with established records retention policies and schedules.</p>	ISG	

## Security Incident Response

### SECURITY INCIDENT RESPONSE (*DETAIL FORM*)

---

The following is a sample incident report. The report is an example of the types of information and incident details that will be used to track and report security incidents for Coconino Community College. The format of this report is subject to change as reporting standards and capabilities are further developed.

#### Contact Information and Incident

Last Name: _____	First Name: _____
Job Title: _____	Alt Phone: _____
Phone: _____	Pager: _____
Mobile: _____	Fax: _____
Email: _____	

#### Incident Description

##### Date/Time and Recovery Information

Date/Time of First Attack: _____	Date: _____	Time: _____
Date/Time of Attack Detected: _____	_____	Time: _____
Has the Attack Ended: _____	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Duration of Attack (in hours): _____		
Severity of Attack: _____	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	
Estimated Recovery Time of this Report (Clock) _____		
Estimated Recovery Time of this Report (Staff Hours) _____		
Estimated Damage Account as of this Report (\$\$\$ Loss) _____		
Number of <b>Hosts</b> Affected: _____		
Number of <b>Users</b> Affected: _____		

##### Type of Incident Detected:

- |   |  |   |  |  |
|---|--|---|--|--|
| <input type="checkbox"/> Exposing Confidential/Classified/Unclassified Data | <input type="checkbox"/> Theft of Information Technology Resources/ Other Assets | <input type="checkbox"/> Creating accounts                | <input type="checkbox"/> Altering DNS/Website/Data / Logs    | <input type="checkbox"/> Destroying Data         |
| <input type="checkbox"/> Anonymous FTP abuse                                | <input type="checkbox"/> Attacking Attackers/ Other Sites                        | <input type="checkbox"/> Credit Card Fraud                | <input type="checkbox"/> Fraud                               | <input type="checkbox"/> Unauthorized Use/Access |
| <input type="checkbox"/> Using Machine Illegally                            | <input type="checkbox"/> Impersonation   | <input type="checkbox"/> Increasing Notoriety of Attacker | <input type="checkbox"/> Installing a Back Door/Trojan Horse | <input type="checkbox"/> Attacking the Internet  |
| <input type="checkbox"/> ICQ Abuse/IRC Abuse                                | <input type="checkbox"/> Life Threatening Activity                               | <input type="checkbox"/> Password Cracking                | <input type="checkbox"/> Sniffer                             | <input type="checkbox"/> Don't Know              |
| <input type="checkbox"/> Other (Specify) _____                              |  |   |  |  |

<b>SB1386</b> – Is Email Notification Required? <input type="checkbox"/> Yes <input type="checkbox"/> No	SB1386 - Email Notification Sent Out? <input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Comments (Specify Incident Details and additional information):

#### General Information

##### How Did You Initially Become Aware of the Incident?

- |  |  |   |   |   |
|--|--|---|---|---|
| <input type="checkbox"/> Automated Software Notification | <input type="checkbox"/> Automated Review of Log Files | <input type="checkbox"/> Manual Review of Log Files | <input type="checkbox"/> System Anomaly (i.e., Crashes, Slowness) | <input type="checkbox"/> Third Party Notification |
| <input type="checkbox"/> Don't Know                      | <input type="checkbox"/> Other (Specify) _____         |   |   |   |

##### Attack Technique (Vulnerability Exploited / Exploit Used)

## Security Incident Response

- |  |   |  |   |
|--|---|--|---|
| <input type="checkbox"/> CVE/CERT VU or BugTraq Number | <input type="checkbox"/> Virus, Trojan Horse, Worm, or Other Malicious Code | <input type="checkbox"/> Denial of Service or Distributed Denial of Service Attack | <input type="checkbox"/> Unauthorized Access to Affected Computer Privileged Compromise (Root/Admin Access) User Account Compromise/Web Compromise (Defacement) |
| <input type="checkbox"/> Scanning/Probing              | <input type="checkbox"/> Other  |  |   |

**Suspected perpetrator(s) or possible motivation(s) of attack:**

- |   |  |   |                                  |
|---|--|---|----------------------------------|
| <input type="checkbox"/> CSU staff/students/faculty | <input type="checkbox"/> Former staff/students/faculty | <input type="checkbox"/> External Party | <input type="checkbox"/> Unknown |
| <input type="checkbox"/> Other (Specify) _____      |  |   |                                  |

### Malicious Code

**Virus, Worm**

Name or Description of Virus \_\_\_\_\_

Is Anti-Virus Software Installed on the Affected Computer(s)?  Yes (Provide Name) \_\_\_\_\_  No

Did the Anti-Virus Software Detect the Virus?  Yes  No \_\_\_\_\_

When was your Anti-Virus Software Last Updated? \_\_\_\_\_

### Network Activity

**Protocols**

Name or Description of Virus \_\_\_\_\_

TCP  UDP  ICMP  IPSec  IP Multicast  Ipv6

Other \_\_\_\_\_

Please Identify Source Ports Involved in the Attack: \_\_\_\_\_

Please Identify Destination Ports Involved in the Attack: \_\_\_\_\_

### Impact of Attack

**Hosts**

**Individual Hosts**

Does this Host represent an Attacking or Victim Host?  Victim  Attacker  Both

Host Name: \_\_\_\_\_ IP Address: \_\_\_\_\_

Operating System Affected: \_\_\_\_\_ Patch Level (if known): \_\_\_\_\_

Applications Affected: \_\_\_\_\_ Database: \_\_\_\_\_

Others: \_\_\_\_\_

Primary Purpose of this Host:

<input type="checkbox"/> User Desktop Machine	<input type="checkbox"/> User Laptop Machine	<input type="checkbox"/> Web Server	<input type="checkbox"/> Mail Server	<input type="checkbox"/> FTP Server
<input type="checkbox"/> Domain Controller	<input type="checkbox"/> Domain Name Server	<input type="checkbox"/> Time Server	<input type="checkbox"/> NFS/File System Server	<input type="checkbox"/> Database Server
<input type="checkbox"/> Application Server	<input type="checkbox"/> Other Infrastructure Services			

**Bulk Hosts**

Bulk Host Information (Details):

Comments (Please detail incident):

**Data Compromised:**

Did the attack result in a loss/compromise of sensitive or personal information?  Yes (Specify)  No  Other

## Security Incident Response

Comments:

Did the attack result in damage to system(s) or data:

Yes (Specify)     No     Other

Comments:

### Law Enforcement

Has Law Enforcement Been Notified?

Yes     No

### Remediation:

Please detail what corrective actions have been taken (specify):

Comments:

## Lessons Learned Information (Optional)

Did Your Detection and Response Process and Procedures Work as Intended?

Comments:

Please provide Discovery Methods and Monitoring Procedures that would have Improved Your Ability to Detect an Intrusion.

Comments:

Are there Improvements to Procedures and Tools that would have Aided You in the Response Process.

Comments:

Are there Improvements that would have Enhanced Your Ability to Contain an Intrusion

Comments:

Are there Correction Procedures that would have Improved Your Effectiveness in Recovering Your Systems.

Comments: