SENSITIVE DATA EXPOSURE INCIDENT CHECKLIST

INCIDENT # _____

Date became aware: _____ Date reported to Security Office: _____ 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 Unit systems administrator and end user, but may also result from proactive incident detection work of the Security Office or central IT operations. If it is determined that an incident has occurred, inform appropriate authorities.

Done	*Task*	*Owner*	*Notes*
	1.1 Immediately contain and limit exposure: - If electronic device has been compromised: o Do not access (do not logon) or alter compromised device o Do not power off the compromised device o Do unplug network cable (NOT power cable) from the compromised device - 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. *RESOURCES:* a) New York University IT Security Information Breach Notification Procedure b) University of Massachusetts Amherst Incident Prevention and Response Procedure	Unit	

	1.2 Alert Security Office immediately *GUIDANCE: Insert appropriate names and telephone numbers, email address, and/or link to online security incident reporting form.* *EXAMPLES:* c) *Call John Smith at 999-999-9999 or Mary Jones at 999-999-9999. If you do not get one of them IN PERSON, then call the Help Desk at 999-999-9999 and have them contact the Information Security Office. Also send details to it-incident@xxxxx.edu* d) *Report incident according to XYZ policy via online form (preferred) or call John Smith at 999-99-9999.* *RESOURCES:* a) *Indiana University Incident Reporting Procedures* b) *University of Virginia Information Security Incident Reporting Policy and online reporting form*	Unit	
	1.3 If the incident involves electronic devices or media stolen or lost within the local community, also alert law enforcement. *GUIDANCE: This sub-step should be included ONLY if advised to do so by your campus police department. Be certain to consult with them on this issue.* *EXAMPLES:* *a) Call Campus Policy Hotline at 999-999-9999* *b) Call E-911 to report the incident. The E-911 service will contact the appropriate city, county, or campus police jurisdiction.*	Unit	
	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: *EXAMPLES:* *a) Executive in charge of IT for the institution, e.g., Vice President/CIO* *b) Executive in charge of organizational unit in which incident occurred, e.g., Vice President, Provost, Dean*	Security Office	

	c) Campus Chancellor/President (or his/her Chief of Staff) *d) Counsel for the institution* *e) Law enforcement, e.g., campus police, FBI local office, Secret Service local office* *f) Public Affairs* *g) Internal Audit* *h) Risk Management* *i) Appropriate Data Steward(s) for the type of data potentially at risk* *j) Health information compliance office, if HIPAA-protected potentially at risk* *k) Vice president for research, if research data potentially at risk* *l) Finance office, if credit card #, bank account #, or other sensitive financial data potentially at risk*		
	1.5 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.		
	STEP 2: DAMAGE CONTAINMENT AND DATA EXPOSURE ASSESSMENT ***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.***		
	2.1 Assemble Incident Response Team *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.*	Security Office	
	2.2 Review incident response process and responsibilities with Incident Response Team - Provide each member with current Sensitive Data Exposure Incident Checklist - Discuss communications strategy - Stress importance of maintaining chain of custody *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*	Security Office	

	the team and appropriate University officials. *EXAMPLES:* *a) Team members must not discuss the incident with anyone outside the team until and only if authorized to do so by the Security Office head.* *b) All documentation created by team members must be fact-based, as it may become important reference or evidence* *c) Daily conference call of team members will be held discuss status.* *d) Instruct team to track time spent on the incident.*		
	2.3 Collect and preserve evidence *GUIDANCE:* *Collect physical and cyber evidence that provides a clear, detailed description of how the sensitive data was compromised.* *EXAMPLES:* *a) Image of hard drive(s)Physical equipment* *b) Network traffic flow to/from compromised device* *c) Workstation and application logs* *d) Access logs* *e) Digital photographs of the evidence and surrounding area* *RESOURCES:* *http://www.educause.edu/Resources/ForensicOverview/161135* *http://www.cybercrime.gov/ssmanual/index.html* *http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf*	Incident Response Team	
	2.4 Establish and maintain appropriate chain of custody for all evidence. *GUIDANCE:* *Inventory pieces of evidence and track who accessed, used, stored, moved or returned each piece of evidence and when it was accessed.* *EXAMPLES:* a) Establish what exactly the evidence is b) Document who handled it and why		

	c) Document where and how it was stored 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 *RESOURCES:* *http://www.cert.org/csirts/services.html* *http://www.sans.org/score/incidentforms/ChainOfCustody.pdf*		
	2.5 Take actions needed to limit the scope and magnitude of the incident *EXAMPLES:* *a) 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, e.g., Wayback Machine* *b) Change passwords that may have been compromised* *c) Cease operation of a compromised application or server*	Incident Response Team	
	2.6 Perform forensics and document findings: a. Analyze evidence b. Reconstruct incident c. Provide detailed documentation *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*	Incident Response Team	
	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	Incident Response Team	
STEP 3: ERADICATION AND RECOVERY ***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***			

	3.1 Revisit 2.4 and look for additional ways to limit exposure *EXAMPLES:* *a) Run web queries periodically to ensure that the data has not been further exposed or cached.* *b) Review the inventory of equipment and systems impacted and change additional passwords that may have been compromised* *c) Cease operation of a compromised application or server and develop work-arounds*		
	3.2 Eradicate and/or mitigate system vulnerabilities, review access privileges and remediate risks to sensitive data stores *EXAMPLES:* *a) Run vulnerability scans on impacted systems;* *b) Review and determine where data resides and make adjustments to ensure increased protection as needed.* *c) Limit access to systems to only those who need it;* *d) Use software tools to find, delete and secure sensitive data, e.g., Identity Finder*		
	3.3 Return evidentiary equipment and systems to service once they are secured.		
STEP 4: NOTIFICATION ***Determine the need to give notice to individuals whose data may have been exposed by the incident. Swiftness 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.***			
	4.1 Make decisions based upon Incident Response Team findings - Does level of exposure risk warrant notification letters? - If yes, • If applicable, has law enforcement authorized notification to affected parties? • Who will issue letter? • Who will handle telephone and email responses to questions from affected	Appropriate institution officials	

	individuals? Does expected volume warrant setting up call center? • Does magnitude of exposure warrant a press release? Incident information website? • Does exposure risk warrant free credit monitoring? - **<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>** *GUIDANCE:* *a) 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.* *b) 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. 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.* *c) See EDUCAUSE Data Incident Notification Toolkit for further guidance.*		
	4.2 Collect name and contact information on affected individuals *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.* *Ensure that data is collected, transmitted and stored securely and removed when it is no longer needed.*	Unit, advised by Security Office	
	4.3 Set up telephone and email support for affected individual questions: - Identify appropriate person(s) to handle calls and emails - Establish telephone call line/routing infrastructure, if not available	Unit, advised by Security	

	- Identify/set up telephone number to use - Identify/set up email address to use - Train individuals handling calls and emails, including providing them with a list of anticipated questions and answers *GUIDANCE: See EDUCAUSE Data Incident Notification Toolkit – FAQ Section for advice and sample content for telephone and email responder FAQs.*	Office	
	4.4 If deemed appropriate by institution officials in Sub-step 4.1, create website for affected individuals - Identify URL and location - Restrict access until ready to go live - Draft content *GUIDANCE:* *a) Incident websites are typically reserved for situations in which contact information for individuals affected by the breach is unknown or incomplete.* *b) See EDUCAUSE Data Incident Notification Toolkit – Website Section for advice and sample content* *c) Website content should be approved by appropriate institution officials, e.g.,* • *Executive in charge of IT for the institution, e.g., Vice President & CIO* • *Executive in charge of organization in which incident occurred* • *Public affairs office* • *Counsel for the institution*	Unit, advised by Security Office	
	4.5 If deemed appropriate by institution officials in Sub-step 4.1, obtain free credit monitoring services for affected individuals *GUIDANCE: 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.*	Unit, advised by Budget and Procurement Offices	
	4.6 If deemed appropriate by institution officials in Sub-step 4.1, prepare press release - Identify contact for media - Compose text for press release - Develop talking points	Public Affairs	

	GUIDANCE: *a) 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.* *b) See EDUCAUSE Data Incident Notification Toolkit – Press Release Section for advice and sample content.* *c) Content should be approved by appropriate institution officials, e.g.,* • *Executive in charge of IT for the institution, e.g., Vice President & CIO* • *Executive in charge of organization in which incident occurred* • *Public affairs office* • *Counsel for the institution*		
	4.7 Prepare notification letter to affected individuals - Identify letter issuer and letterhead to be used - Compose draft text *GUIDANCE:* *a) See EDUCAUSE Data Incident Notification Toolkit – Letter Section for advice and sample content.* *b) Letter content should be approved by appropriate institution officials, e.g.,* • *Executive in charge of IT for the institution, e.g., Vice President & CIO* • *Executive in charge of organization in which incident occurred* • *Public affairs office* • *Counsel for the institution*	Unit, advised by Security Office	
	4.8 Prepare mailing of notification letters (postage, addresses) - Finalize address information - Arrange for mail merge and printing/stuffing` of letter and envelopes *GUIDANCE: Avoid personalizing each letter with the affected individuals name, as this increases the risk of mismatched letters and envelopes*	Unit	
	4.9 If required by state law, notify the State's Attorney General within the required notification timeframe	University Counsel or other designated	

		office	
	4.10 Notify appropriate Federal agency as required by law *EXAMPLES:* *a) U.S. Department of Education when FERPA-protected student data is exposed* *b) U.S. Department of Health and Human Services when HIPAA-protected medical data is exposed* *RESOURCES:* *HIPAA: http://www.hhs.gov/ocr/privacy/* *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html* *FERPA: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html* *Other data protection laws, http://protect.iu.edu/cybersecurity/data/laws*	University Counsel or other designated office	
	4.11 Notify granting organizations and research partners if research data compromised, as dictated by contractual obligations	University Counsel or designated office	
	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. *EXAMPLES:* *a) Employee benefit vendors* *b) Student services vendors*	Unit	
	4.13 If Credit Card data exposed, notify the credit card processor(s) or merchant banks *GUIDANCE: Specific notification requirements are governed by the card brand.* *EXAMPLE:* *VISA -- http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html* -	Treasurer	
	4.14 Notify Credit Bureaus as required by State and upon consultation with University Council	Treasurer with advice from	

		University Counsel	
	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.	Unit, Security Office, University Counsel, and Public Affairs	
	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.	Data Custodian	
STEP 5: FOLLOW-UP ***Identity lessons learned from the incident, implement any remediation needs, and securely store a complete record of the incident.***			
	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 Security Office	
	5.2 Schedule a debriefing meeting two to six weeks afterwards to review what could have been done better in responding to the incident.	Security Office, Public Affairs, University Counsel, and appropriate others	
	5.3 Assess remediation needs - Issue report to unit manager and executive management if appropriate - Follow up to ensure completed	Security Office	

	EXAMPLES: *a) Why was the data stored in a vulnerable place?* *b) What more could have been done to avoid the intrusion?* *c) Is the unit taking appropriate steps to remediate?*		
	5.4 Initiate plans and projects to implement remediation needs. - Apply lessons learned and recommended changes to access, sensitive data stores, systems and processes to increase protection	Unit	
	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.	Security Office	