IT PRACTICE PROCEDURE

Security Incident Response Plan

All computer incidents should be reported and analyzed to determine the scope and severity. Evidence of an unauthorized intrusion of a system via an individual or via malicious code must be carefully reviewed especially if that system contains any regulated, confidential or sensitive information.

Effective as of: **7/1/2013**

Sponsor and Approvers:

J. Ashley Ewing, UA Chief Information Security Officer

John McGowan, UA Chief Information Officer; Scott Montgomery, UA Deputy Chief Information Officer

Status of Guideline: **Approved for publication**

Audience:

This IT Procedure should be observed by:

OIT Technology Practitioners ☒

All Technology Practitioners ☒

Contractors/suppliers ☒

Other (specify) ☒ HIPAA Business Associates; Third Party Hosting providers

Statement of need and purpose:

Regulatory requirements and security best practices require an Incident Response Plan for appropriate management and documentation of all security incidents.

Procedure:

Introduction

All incidents at the University of Alabama should be reported and investigated to determine if the information data involved requires an official notification of exposure as determined by regulation or contract. Failure to report could result in individual disciplinary action, additional fines from regulatory entities, and/or loss of trust in the University by the community at large. An incident can be any unauthorized access to confidential or sensitive data through:

- A computer hacking incident
- A virus or malware incident including ransomware
- The loss of any mobile computing device (e.g. laptop, tablet, phone) and/or mobile storage device (e.g. thumb drive, external drive, CD/DVD) that contains confidential or sensitive data
- Any unauthorized access, or downloading of confidential or sensitive data either by an individual with approved access or without approved access

Depending on the data involved, one or more regulatory entities and/or affected individuals will require prompt notification. An incident form like the ones referenced in this document should always be completed to track and manage all incidents.

Responding to a Breach

The check list below provides current best practice for responding to a security breach. The items in the checklist are not linear in nature as some activities may occur in parallel. This checklist should be used for a breach of personally identifiable information (PII), electronic protected health information (ePHI – HIPAA), credit card data (Payment Card Industry Data Security Standards – PCI DSS), educational records (Family Educational Rights and Privacy Act – FERPA), research data, or other sensitive data. Document your findings in the Incident Response Form.

- ***Validate the data breach***
  - Do not assume that every identified incident is actually a breach of sensitive data as referenced in the paragraph above or described in this document
  - Examine the initial information and available logs to confirm that the breach has occurred
  - If possible, Identify the type of information disclosed and estimated method of disclosure (internal/external disclosure, malicious attack or accidental)

- ***Once a breach has been validated, immediately assign an incident manager to be responsible for the investigation***
  - Assign a senior level manager, such as the Chief Information Security Officer or an individual at an equivalent director level position, to serve as an incident manager to coordinate multiple organizational units and the overall incident response. (Typically, the team manager is the incident manager; alternatively, the team manager assigns another individual to lead the response activities.)
  - Begin breach response documentation and reporting process using the Incident Response Form
  - Coordinate the flow of information to appropriated senior leadership and manage public communications about the breach with University Strategic Communications as defined below in “Notification Determination and Notification Process”

- ***Assemble incident response team***

- Include representatives as appropriate from management, information technology, legal, university relations, risk management, finance, and audit departments (and possibly HR, for internal incidents) in the incident response team
- Immediately determine the status of the breach (on-going, active, or post breach).
- If the breach is active or on-going, take action to prevent further data loss by securing and blocking unauthorized access to systems/data and preserve evidence for investigation
- Document all mitigation efforts for later analysis in the Incident Response Form
- Advise staff who are informed of the breach to keep breach details in confidence until notified otherwise

€ ***Determine the scope and composition of the breach***

- Notify, as early as possible, the University of Alabama System (UAS) Office of Risk Management to determine the reporting to our Cyber Insurance Provider. The Cyber Insurance Provider is interested in the following reporting requirements:
    1. Any lawsuit related to a cyber incident
    2. Demand for damages (for example, letter from lawyer, etc.)
    3. Regulatory notice or investigation alleging activities (or failures to act) related to our information services
    4. Hiring or retaining external resources/consultants to help with response to an event, breach, etc.
    5. Any event disclosing records containing PHI or PII of **100 or more individuals**
    6. Any cyber extortion demand
    7. Network interruption of 12 hours or more triggered by or involving an intrusion or unauthorized access
    8. Any significant event that may result in expenses **greater than $100,000**
    9. Any event that is expected to, or does, receive adverse media attention or inquiries
- Use the UAS Office of Risk Management "Information Security Event Reporting Form" to document an incident for the Cyber Risk Insurance provider
- Consult your legal counsel to examine any applicable federal, state, and local breach reporting requirements to determine which additional authorities or entities must be notified in order to satisfy compliance requirements.
- Seek involvement of law enforcement when there is a reason to believe that a crime has been committed or to maintain compliance with federal, State, or local legal requirements for breach notification.
- If criminal activity is suspected, notify UAPD and any applicable federal, state, or local legal requirements relating to the notification of law enforcement. (The decision to involve outside entities, including external law enforcement, should generally be made in consultation with executive leadership and UA legal counsel).
- Identify all affected data, machines, and devices
- Conduct interviews with key personnel and document facts (if criminal activity is suspected, UAPD will coordinate these interviews and include any appropriate external law enforcement).

- When possible, preserve evidence (backups, images, hardware, etc.) for later forensic examination. To ensure proper handling of digital evidence, include either UAPD and/or UA OIT forensic team.
- Locate, obtain, and preserve (when possible) all written and electronic logs and records applicable to the breach for examination.
- In concert with executive leadership and legal counsel, designate a single organizational representative (typically incident manager) authorized to initiate and/or communicate breach details to any party, including law enforcement.

€ ***Notify the data owners***

- Reach out to data owners as soon as possible to notify them about the breach
- Foster a cooperative relationship between the incident response team and data owners
- Work collaboratively with data owners to secure sensitive data, mitigate the damage that may arise from the breach, and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences

€ ***Decide how to investigate the data breach to ensure that the investigative evidence is appropriately handled and preserved***

- Decide in advance whether you will investigate a potential breach using in-house resources or an outside service provider
- Seek advice from UAPD and/or the UA OIT Forensic team on the approved methods for protecting digital evidence, so that you are prepared and are able to properly preserve and document all evidence to ensure it can be used in a court of law, if necessary. This requires detailed recording and following proper collection, handling, storage, custody documentation, and destruction procedures (if applicable).
- If law enforcement is involved, collaborate with them to help ensure that any other in-house investigations do not interfere with law enforcement activities
- Once investigative activities have been completed, safely store, record, and/or destroy (where appropriate) all evidence
- Consider all alternatives to replacing or clearing compromised resources and machines, including the cost of remediation or rebuilding of the assets to an acceptable security level

€ ***Determine whether notification of affected individuals is appropriate and, if so, when and how to provide such notification***

- Determine whether notification is warranted and when it should be made as defined in the “Notification Determination and Notification Process” section below. Executive leadership at the senior technical and/or administrative level, in coordination with legal counsel, is the authority that should generally make this final decision.
- Notify affected individuals whose sensitive information, including PII, has been compromised, as required by applicable federal, state, and local laws
- Provide notification in a straightforward and honest manner; avoid evasive or incomplete notifications

- If the breach represents a threat to affected individuals' identity security, consider providing credit monitoring or identity theft protection services to mitigate the risk of negative consequences for those affected
- Make every attempt to avoid news of the breach reaching the media before you notify affected individuals
- Work closely with University Relations staff to craft the appropriate media notification (mailings, emails, phone calls, etc.).

€ ***Collect and review any breach response documentation and analyses reports***

- Assess the data breach to determine the probable cause(s) and minimize the risk of future occurrence
- Address and/or mitigate the cause(s) of the data breach
- Solicit feedback from the responders and any affected entities.
- Review breach response activities and feedback from involved parties to determine response effectiveness
- Make necessary modifications to your breach response strategy to improve the response process
- Enhance and modify your information security and training programs, which includes developing countermeasures to mitigate and remediate pervious breaches; lessons learned must be integrated so that past breaches do not reoccur.

Specific Examples of Sensitive Data:

Credit Card/Debit Card Data (PCI DSS)

All systems that transmit, process, or store cardholder information (credit card/debit card) is governed by the Payment Card Industry Data Security Standards (PCI DSS). The University PCI Compliance Committee will oversee the management of payment card incidents lead by the University Information Security Officer (ISO).

Once it is determined that a breach has occurred that involves the possible exposure of cardholder data, the PCI Compliance Committee will begin the documentation for the notification process which may include any or all of the following:

- The incident form referenced in this document should be completed for tracking and management
- Within 3 business days of the reported incident, the PCI Compliance Committee will provide an Incident report to the University Merchant Services Bank (TouchNet+Heartland, or any others)
- Through coordination with the University merchant services bank, the PCI Compliance Committee will follow the breach notification instructions on each of the card providers' web sites (Visa, Master Card, Discover, American Express, etc.)
- It is extremely important for the University merchants to notify OIT Security and the PCI Compliance Committee of any incidents on systems that process, transmit or store card holder

information – failure of the University to promptly notify our merchant service providers and, as directed, the card providers could lead to extensive fines for the University

- Report any breach affecting 100 or more individuals to the University of Alabama System (UAS) Office of Risk Management to provide reporting to our Cyber Risk Insurance provider.

Once an appropriate amount of incident data and facts are known, representatives from the PCI Compliance Committee investigation will begin meetings as described below related to the Notification Determination and Notification Process procedures.

Protected Health Information (HIPAA)

All protected health information (PHI) covered under the Health Insurance Portability and Accountability Act (HIPAA) for any University acknowledged HIPAA entities or HIPAA Business Associate (BA) entities is governed by HIPAA regulations. The University HIPAA Privacy Officer, University HIPAA Security Officer and/or University Information Security Officer will oversee the management of PHI security incidents along with the Security Officer and/or Privacy Officer for the HIPPA entity/HIPAA Business Associate entity.

NOTE: Privacy related PHI incidents are normally managed by the HIPAA entity Privacy Officer/HIPAA entity Security Officer in accordance to HIPAA privacy policy. The privacy investigation team will notify the University HIPAA Security Officer and University Information Security Officer as necessary during the investigation process.

Each HIPAA entity should maintain a log of all know breaches of unsecured protected health information. It is a requirement to notify the Secretary of HHS of all breaches of unsecured protected health information that affect fewer than 500 individuals during a calendar year. The notification must be submitted no later than 60 days after the calendar year during which the breach occurred, in other words by March 1. The notification must be submitted electronically by the HIPAA entity Privacy or Security Officer using a form posted on the website of the Office of Civil Rights.

If a breach of PHI affects 100 or more individuals, work with the University of Alabama System (UAS) Office of Risk Management to provide reporting to the Cyber Risk Insurance provider.

If a breach affects 500 or more individuals, a covered entity must provide the Secretary with notice of the breach without unreasonable delay and in no case later than 60 days from discovery of the breach. The notification must be submitted electronically by the HIPAA entity Privacy or Security Officer using a form posted on the website of the Office of Civil Rights.

Once it is determined that a security breach has occurred that involves the possible exposure of unsecured PHI, the entity HIPAA Security Officer along with the University Information Security Officer will begin the documentation for the notification process which may include any or all of the following:

- The entity HIPAA Security Officer and/or entity HIPAA Privacy Officer will fill out the HIPAA incident form to document the incident and notification process

- The discovery and 60 day notification requirement begins on the first day a breach is known by the covered entity or business associate of the covered entity
- In the case of an unauthorized exposure/breach of unsecured PHI, the HIPAA cover entity is required to notify without reasonable delay, and in no case, later than 60 days of discovery each individual involved
- In the case of an unauthorized exposure/breach of unsecured PHI, the business associate of a covered entity must immediately (within 24 hours) notify the covered entity
- Notice to an individual shall be provided promptly and in the following form:
    - Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available.
    - As defined by HIPAA Regulation: "In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual), electronic notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period determined by the Secretary of Health and Human Services on the home page of the Web site of the covered entity involved or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured PHI is possibly included in the breach."
    - If imminent misuse of unsecured PHI is deemed possible by the covered entity, in addition to notice provided as described above, the covered entity involved, may also provide information to individuals by telephone or other means, as appropriate.
    - Media Notification – For breaches involving unsecured PHI of more than 500 residents of such state or jurisdiction, notice shall be provided to prominent media outlets serving a state or jurisdiction
- NOTE: the term ''unsecured protected health information'' is PHI that is not secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute (ANSI). This is normally accomplished through encryption techniques for electronic media (laptops, thumb drives, CD/DVD, backup data, etc.), or physical destruction via cross cut shredding, pulping or incineration.

Once an appropriate amount of incident data and facts are known, representatives from the HIPAA investigation will begin meetings as described below related to the Notification Determination and Notification Process procedures.

Educational Records (FERPA)

All educational records covered under the Family Educational Rights and Privacy Act (FERPA) is governed by the FERPA regulations. The University Registrar will oversee the management of FERPA related events with as needed assistance from the University Information Security Officer.

Once it is determined that a security breach has occurred that involves the possible exposure of unsecured student information, the Dean(s) of the College(s), or Vice President(s) involved along with the University Registrar and, if needed, University Information Security Officer will begin the documentation for the notification process which may include any or all of the following:

- The incident form referenced in this document should be completed to tracking and management
- All FERPA notifications will be made from the College/Vice Presidential organization involved to the Family Policy Compliance Office, and will include:
- Date of the incident
- Date of discovery of the incident
- Brief description of the incident
- Description of the student information involved and number of students affected
- Corrective measures that will prevent the incident from occurring again
- Risk to the individual caused by the incident
- UA contact for further information or assistance
- If confidential data was involved such as name with Social Security Number, etc., a separate notification will be made to the individuals affected as described in this document

Once an appropriate amount of incident data and facts are known, representatives from the FERPA investigation will begin meetings as described below related to the Notification Determination and Notification Process procedures which may include:

- ***Notifying FPCO and seeking technical assistance from PTAC***
    - Consider notifying Family Policy Compliance Office (FPCO) about the breach. (FERPA does not require that you notify FPCO of the breach; however, the U.S. Department of Education considers it a best practice. While FPCO has the discretion under 34 CFR §99.64(b) to conduct its own investigation of a breach, it will take into consideration an effort to proactively come into compliance demonstrated by voluntarily notifying FPCO about the breach.) FPCO can assist educational agencies and institutions by
        - ✓ helping to determine the potential for harm resulting from the release of the information; and
        - ✓ Assisting with coming into compliance with FERPA.

    - After notifying data owners about the breach, consider seeking technical assistance from PTAC for informal help with security and breach prevention. PTAC can assist educational agencies and institutions by
        - ✓ providing real-word advice and best practices for responding to privacy and security incidents, notification, and data recovery;

- ✓ Assisting technical staff in conducting investigation and fact-finding activities; and
- ✓ Helping organizational decision-makers with developing a strategy for incident mitigation and data recovery.

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) includes individual names along with social security numbers, address, date-of-birth, drivers' licenses numbers, and other personal information. The University Information Security Officer will oversee the management of PII incidents along with the appropriate Dean/Vice President associated with the data in the incident.

Once it is determined that a security breach has occurred that involves the possible exposure of unsecured PII, the Dean(s) of the College(s), or Vice President(s) involved along with the University CIO and, the University Information Security Officer will begin the documentation for the notification process which may include any or all of the following:

- The incident form referenced in this document should be completed to tracking and management
- Date of the incident
- Date of discovery of the incident
- Brief description of the incident
- Description of the PII involved
- Corrective measures that will prevent the incident from occurring again
- Risk to the individual caused by the incident
- Steps individuals should take to protect themselves
- UA contact for further information or assistance

If a breach of PII affects 100 or more individuals, work with the University of Alabama System (UAS) Office of Risk Management to provide reporting to the Cyber Risk Insurance provider.

Once an appropriate amount of incident data and facts are known, the representatives from the PII investigation will begin meetings as described below related to the Notification Determination and Notification Process procedures.

Protected Research Information

Protected research information includes information under a specific "Data Use Agreement" or any other data management/data security plan related to research as defined by the disclosure requirements in the grant, research proposal or research contract. The University Information Security Officer will oversee the management of protected research information incidents along with the

Institutional Review Board (IRB) or other research oversight group, and the appropriate Dean/Vice Presidents associated with the data in the incident. While most of this information is de-identified, the notification requirements may only be to the provider of the research data. In other situations, data is not de-identified and unauthorized exposure would be considered a breach requiring individual notification.

Once it is determined that a security breach has occurred that involves the possible exposure of Protected research information, the Dean(s) of the College(s), or Vice President(s) involved along with the University CIO and, the University Information Security Officer will begin the documentation for the notification process. The process will follow the breach notification requirements defined in the specific "Data Use Agreement" or any other data management/data security plan included in the research grant/contract. If no specific guidelines are provided, then the procedures for PII should be followed for the notification of individuals' personal information.

Once an appropriate amount of incident data and facts are known, representatives from the research data investigation will begin meetings as described below related to the Notification Determination and Notification Process procedures.

Non-Criminal Investigation

Non-Criminal Investigations are inquiries internal to the University that do not initially appear to be related to the commission of a crime. These are usually as eDiscovery request from the Office of Counsel. The University Certified Forensic Analyst will conduct the review of the data request and provide the resulting reports back to the Office of Counsel. The University Information Security Officer will assist as requested by the Office of Legal Counsel.

Notification would only be required if during the investigation, unauthorized exposure of confidential data was discovered. In that situation, the appropriated processes in this document would be followed based on the data involved.

Viruses, Malware, Intrusions, Ransomware, Compromised Systems

Systems that do not contain any of the sensitive, confidential or regulated data mentioned above, but have been involved in an incident, will be handled as follows.

- Where possible, the state of the antivirus client and virus signature files should be determined and documented
- Where possible, the state of the patch level for the operating system should be determined and documented
- Where possible, the state of the client release and patch level for certain key applications should be determined and documented (e.g. Windows Office applications, Adobe Applications, Internet Explorer, Chrome, Mozilla, Safari Browsers, Java release level)

- Where possible, pull the contents of the users browser history files should be pulled and documented
- Tools should be used to identify and eradicate the unauthorized virus, malware and associated malicious code and document the findings from the tool (Full virus scan, Malwarebytes scan, other tools such as Combo Fix, etc., including runs in safe mode)
- In many cases, remediation of the problem may result in the complete reloading of the system involved in the incident
- Document via trouble ticket information above and classify as a virus removal for metric tracking

Systems that have been compromised such as servers or web sites should determine the possible root cause and perform the following:

- Document all actions taken during the remediation process
- When possible, scan for known vulnerabilities (OIT can assist)
- Pull all access log data for review
- Determine any missing patches in the operating system or applications which may have allowed access through a known vulnerability
- Determine if any compromised user, system or application accounts were used as an entry point
- Determine if the incident is the result of internal unauthorized access (if so, report to HR and OIT security for investigation)

Remediate the problem by removing any unauthorized accounts or applications associated with the compromise, or reload the system from a trusted backup to a trusted state. Next, update software releases, and implement missing security patches. Reset any compromised user, system or application account passwords. Document the incident for metrics tracking.

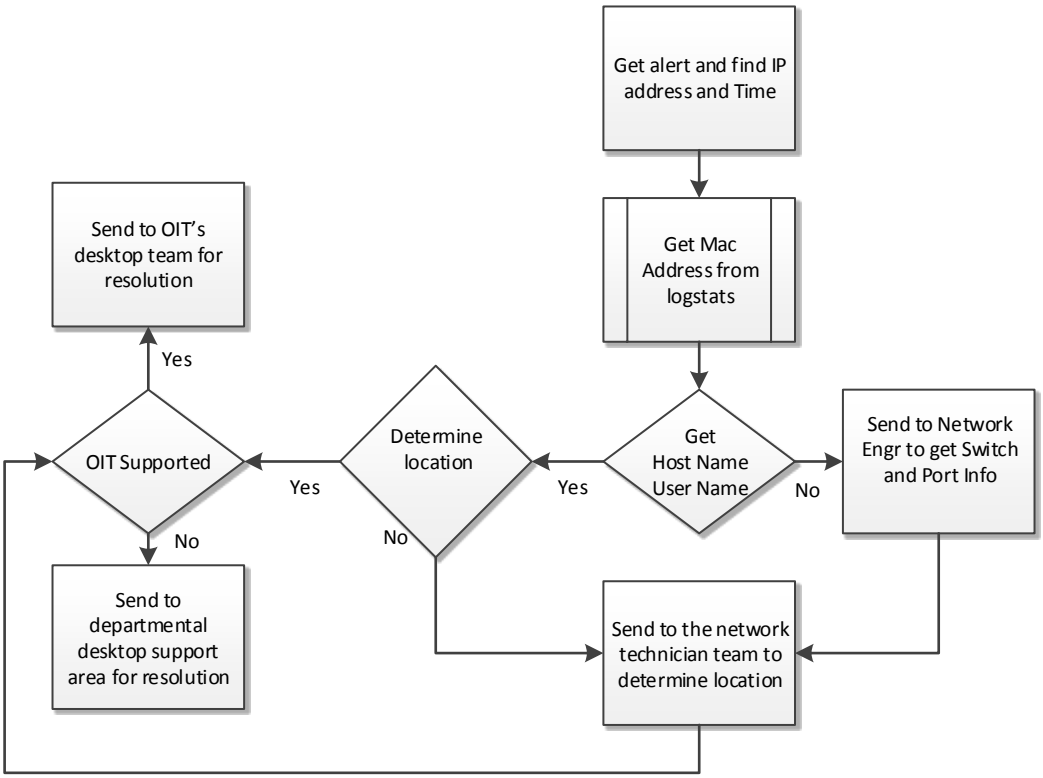
Additional Processes to Assist in the Analysis and Response:

Flowchart to Determine Location of Suspect Machines

In most cases, incidents start with an IP address and a timeframe. This information can come from several locations:

- User trouble ticket
- University abuse email list (abuse@ua.edu)
- REN-ISAC notification list (Research and Educational Networking Information Sharing and Analysis Center)
- University antivirus systems, Firewalls, Intrusion Detection Systems, or other security devices
- Other external notification processes – FBI Bulletins, Security Operations Centers, other Universities or corporations

Once the IP address and time is obtained from a reliable source, log files will be searched to determine the MAC (media access control) address and an attempt will be made to determine the host name and/or user name to determine the physical location of the device. If the host/user name cannot be determined, network engineering will be engaged along with the network technician team to determine the location and ownership of the device. Once ownership is determined, the request is sent to the proper desktop support organization either in OIT or to the user's departmental desktop support team.



Technical Security Assessment Process

Upon discovery of an incident, begin a technical investigation to immediately contain and limit the exposure as much as possible. Steps to contain and preserve evidence to facilitate the investigation:

- Contact the OIT Security group to work with you on the investigation
- Always utilize all Chain of Custody processes and documentation as equipment and information changes hands
- Notify law enforcement for criminal cases (UAPD, FBI, Secret Service, TPD)
- Keep detail logs of all actions taken from the discovery of the incident, and during the investigation and remediation

- The incident form referenced in this document should be completed for tracking and management
- If the incident is a compromised system and the threat is active or the exposure still exist, do not access or alter the compromised system(s) – do not log on at all to the machine and change passwords, do not log in as root, isolate the compromised systems from the network by unplugging the network cable
- Preserve all logs and electronic evidence
- If the systems are on a wireless network and the threat is active or the exposure still exist, isolate the machine from the network by invoking a Wi-Fi kill switch to disable the radio, or by changing the SSID on the access point if possible
- Be on high alert and monitor all systems with any other confidential data (cardholder data, HIPAA, research, etc.)

Gather all available information as quickly and thoroughly as possible. The team should include:

- Representatives from the University security organization
- Any representatives from the technical support organization responsible for the system(s) and/or data involved (either University support or external support)
- Any other required internal or external expertise (network engineers, firewall engineers, intrusion detection/prevention engineers, system administrators, database administrators, data stewards, functional user experts, etc.).

An incident report should be managed throughout the process. Incident Response forms are located on the OIT web site under Information Security in the Incident Response section. HIPAA has its own form, but other incidents can use the generic Incident Response form. Chain of Custody forms are also available at this location and should be used when any systems or data changes hands from owners to investigators. Communications of the incident should be limited to those with a need to know. Regular reporting should occur to the Cyber Incident Response Team (CIRT), and should include the following:

- Initial report on the incident: system(s) involved, data involved, possible causes, status of systems (active, inactive, online, offline, etc.), users affected
- Status reports as necessary: 2-3 times per day initially, daily or during predetermined intervals going forward
- Interim reports will be needed to discuss the scope to the Notification Determination and Notifications Communications team.
- Final report of all known facts related to the incident: system(s)/data, access opportunity, actual data accessed and/or stolen, when, how, by whom, accessed for how long, entry method, root cause, remediation of incident, current status of systems and data, any other information pertinent to the incident and investigation.
- System and data clean up and restoral

Notification Determination and Notification Process

Any investigation of an incident that involves regulated data (PCI DSS, HIPAA, FERPA), or Personally Identifiable Information (PII) such as names with social security numbers must convene the appropriate members of the Cyber Incident Response Team (CIRT) and use the following procedures to determine if notification is required based on the evidence from the incident, and must follow the incident notification process.

- Determine if regulated data and/or PII involved in the incident
- Determine if the regulated data and/or PII were stolen or copied by the unauthorized access
- If it cannot be determined that the regulated data and/or PII were stolen or copied, was the opportunity present to access the data
- If there is indisputable evidence that the regulated data and/or PII was not stolen, copied or accessed, the team should discuss and reach a consensus on the need for notification
- If not, the team should determine the steps and timing for the notification as defined by regulation or based on the specific situation

The CIRT will include the following and others as needed:

1. University Strategic Communications (required)
2. Office of Counsel (required)
3. University Chief Information Security Officer (required)
4. Vice Provost and Chief Information Officer (required)
5. Dean/Vice President organization associated with the data in the incident (required)
6. UA Risk Management Team and/or UA System Office of Risk Management (required)
7. Associate Vice President, Finance (as needed)
8. University of Alabama Police Department (as needed)
9. University Research (as needed)
10. Human Resources (as needed)
11. Registrar (as needed)
12. UA HIPAA Privacy Officer (as needed)

CIRT Incident Communication and Notification

Initial incident data and communications should be restricted to the technical investigation group, University Strategic Communications, the Vice Provost and Chief Information Officer (CIO), the University Chief Information Security Officer (CISO), and the Dean/Vice President associated with the data involved.

Once an appropriate level of pertinent data and facts are available, all appropriate members of the CIRT will convene to discuss and recommend next steps.

All communications will be managed and coordinated through the University Strategic Communications office. The communications will vary as necessary depending on the regulatory entity requirements, the nature of the exposure, and/or the data involved.

Communications should generally include:

- Date of the incident
- Date of discovery of the incident
- Brief description of the incident
- Description of the sensitive data involved
- Corrective measures that will prevent the incident from occurring again
- Risk to any individuals caused by the incident
- Steps individuals should take to protect themselves
- UA contact for further information or assistance

Compliance:

Compliance to this procedure is mandatory within the University to ensure proper handling of security related incidents that may involve regulated, confidential or sensitive data.