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 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:
IT Guidance - Guideline

- A computer hacking incident
- A virus or malware incident
- 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.

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 (BBVA Compass Bank, 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

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 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
IT Guidance - Guideline

- 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.

**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

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, 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.

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. Communications of the incident should be limited to those with a need to know. Regular reporting should occur to the oversight group managing the incident for the University, 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

**Incident Communications**

Initial communications of the Incident should be restricted to the technical investigation group, the University Security Officer, and the Dean/Vice President associated with the data involved.
Communications related to any official notification to employees or external entities will be coordinated through the notification process and notification communications team. This team will include the Office of Counsel, University Relations and the Dean/Vice President organization associated with the data in the incident. The communications will vary as necessary depending on the regulatory entity requirements, the nature of the exposure, and/or the data involved. 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 should 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

### 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 an incident notification team 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 incident notification team will include the University Information Security Officer, a representative from the Office of Counsel, a representative from University Relations, the Dean or Vice President (or their appointed representative) from the area associated with the data in the incident. The University Registrar will also be included for incidents that involve FERPA data.
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.