Reasonable Security and Breach Investigation Procedures and Practices for Public Institutions of Postsecondary Education

Adopted by CPE: February 13, 2015

Background

The *Personal Information Security and Breach Investigation Procedures and Practices Act*, enacted in the 2014 Regular Session, also known as House Bill 5 or the "Cyber Security Bill," requires state and local governments to implement policies and procedures to protect confidential, sensitive personal information and notify individuals if their information has been compromised.

As such, KRS 61.932(1)(b) requires that Kentucky public colleges and universities (hereinafter referred to as "institutions") establish and implement "reasonable security and breach investigation procedures and practices" in accordance with policies established by the Council on Postsecondary Education. KRS 61.931(8) defines "reasonable security and breach investigation procedures and practices" as "data security procedures and practices developed in good faith and set forth in a written security information policy."

The Council's polices for institutional "reasonable security and breach investigation procedures and practices" are set forth below.

Data Security

KRS 61.932(1)(a) states that "an agency that maintains or otherwise possesses personal information, regardless of the form in which the personal information is maintained, shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches." KRS 61.931(6) defines "personal information" as follows:

> An individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
> (a) An account number, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
> (b) A Social Security number;
> (c) A taxpayer identification number that incorporates a Social Security number;
> (d) A driver's license number, state identification card number, or other individual identification number issued by any agency;
> (e) A passport number or other identification number issued by the United States government; or
> (f) Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g.

KRS 61.933(5) states that the notification of security breach provisions shall not apply to personal information in certain circumstances, including that which “is publicly and lawfully made available to the general public from federal, state, or local government records.” As such, the Council does not consider the Security Breach Investigation and Response Procedures and Practices to apply to personal information listed in KRS 61.933(5).

Institutions shall control, maintain and transfer physical and electronic media containing personal information utilizing measures that protect against unauthorized access. As such, institutions shall adopt procedures and practices for data security that, at a minimum, address the areas set forth below and any other requirements by state or federal law:

- Access Control – Only authorized individuals shall be permitted access to personal information. Institutions shall determine the requirements for access to personal information and designate responsibility for making those decisions.
- Acceptable Use – Institutions shall identify acceptable uses of personal information.
- Audit and Accountability – Institutions shall maintain processes in order to monitor and determine system vulnerabilities and implement measures to remediate identified vulnerabilities.
- Security Measures– Security measures shall be implemented in order to prevent unauthorized access or disclosure of personal information. Depending on the media involved (i.e., electronic versus physical), these security measures may include, but are not limited to: password protection, user identification/authentication procedures, encryption, de-identification procedures, firewalls, system security agent software, data destruction procedures and physical access controls.
- Data Classification – Institutions shall maintain a process for classifying data for security purposes in order to determine what security measures, if any, will be implemented in order to protect against unauthorized access or disclosure.
- Risk Assessment/Data Classification – Sensitivity of personal information shall be assessed and classified so that appropriate security measures may be instituted commensurate with the risk of unauthorized disclosure.
- Awareness and Training – Information should be made readily available to users on what constitutes personal information, its acceptable uses, and responsibilities related to its access and notification regarding a potential security breach.
- Sanctions – Institutions shall implement appropriate sanctions in accordance with the Institution’s policies, procedures and guidelines for user violations of applicable data security policies.

<u>Data Security Breach Investigation and Response Procedures and Practices</u>

KRS 61.931(9) defines a “security breach” as follows:

1. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals; or

2. The unauthorized acquisition, distribution, disclosure, destruction, manipulation or release of encrypted records or data containing personal information along with the

> confidential process, or key to unencrypt the records, or data that compromises - or the agency or nonaffiliated third party reasonably believes - may compromise the security, confidentiality or integrity of personal information and result in the likelihood of harm to one (1) or more individuals.

> "Security breach" does not include the good-faith acquisition of personal information by an employee, agent, or nonaffiliated third party of the agency for the purposes of the agency if the personal information is used for a purpose related to the agency and is not subject to unauthorized disclosure.

In the event of a potential security breach or incident, institutions shall follow a plan to identify an incident and respond appropriately. An institution shall adopt procedures and practices for security breaches that, at a minimum, address the areas listed below and any other applicable requirements of state or federal law.

Overview
The steps involved in handling an information security incident can be categorized into five (5) phases:

1. Preparation, Identification and Assessment
2. Containment
3. Eradication
4. Remediation/Recovery
5. Post-Incident Activities and Lessons Learned

Definitions

I. Information Security Incident - any real or suspected event, accidental or intentional, which may compromise the security of personal information. Examples of incidents include:
   a. Attempts (either failed or successful) to gain unauthorized access to personal information.
   b. Theft or other loss of a laptop, desktop, smartphone or other device that contains personal information, whether or not such device is owned by the institution.
   c. The unauthorized or inappropriate use of a system or device for the viewing, transmitting, processing or storing of data.
   d. Changes to system hardware, firmware, or software characteristics without the owner’s knowledge, instruction or consent.

II. Information Security Incident Response Team (ISIRT) – members of the response team who triage, resolve, classify and track information security incidents for the institution. The ISIRT assists in the coordination of efforts by external resources, such as law enforcement agencies and other institutions.

Preparation, Initial Identification and Assessment
Preparation for an information security incident is key to enabling an institution to react quickly and appropriately once an incident is suspected in order to minimize any negative impact. Those with access to personal information should know what constitutes an information security incident, as well as what actions to take should one occur. Institutions should continuously monitor potential threats and learn how to eliminate or mitigate them. Roles and responsibilities should be outlined and communicated to institutional staff, particularly those who may serve as an initial point of contact for the reporting of an incident and on an ISIRT.

When an individual at an institution identifies an information security incident, he or she shall take steps to immediately stop or contain the suspected breach, if possible. After any appropriate initial containment activities by the individual have been completed, he or she shall immediately report the incident as indicated by the institution and further immediate steps may be taken to stop or contain the suspected breach.

When an information security incident is reported, the responsible individual(s) at the institution shall conduct an initial investigation to determine if an information security incident has occurred. As part of the investigation, immediate steps should be taken to minimize the potential for further disclosure of personal information as necessary, including the restriction of information system access or operations. This initial investigation should be brief, but substantive enough to determine if an information security incident has occurred.

If after the initial investigation it is determined that an information security incident has not occurred, the responsible individual shall document both the event and his or her investigative efforts, and close the matter.

If it is determined after initial investigation that an information security incident has occurred, institutions shall complete a full investigation and assessment of the incident, which may include convening the ISIRT. Representatives comprising the team may vary depending on the nature of the personal information breach; however, at a minimum the ISIRT should include representatives from legal, information technology and public information/media relations.

Duties of the ISIRT shall include, as applicable:

- Identifying individuals affected by the breach.
- Determining exactly what personal information has been compromised and its classification (i.e., level of sensitivity).
- Determining the likely impact of the compromised data’s exposure.
- Ensuring that all appropriate actions are immediately taken to prevent any further unauthorized exposure of personal information.
- Fully investigating of the incident, which may include interviewing relevant individuals to learn about the circumstances surrounding the incident and reviewing logs, tapes or other resources.
- If necessary, identifying and engaging consultants, as required to assist the institution in its investigation and/or risk analysis.
- Conducting a root cause analysis of the security breach.
- Within 72 hours of the determination that a security breach has occurred, notifying the commissioner of the Kentucky State Police, the Auditor of Public Accounts, the Attorney General and CPE in accordance with KRS 61.933 on the form prescribed in 200 KAR 1:015.
- Developing a mitigation plan to prevent any further exposure of personal information and risk of harm to anyone affected by the incident, which may include revision of the institutional policies and additional training.
- Determining the appropriate notification requirements and developing an action plan for the delivery of such notices.
- Ensuring compliance at all times with applicable legal and regulatory requirements.
- Keeping institutional leadership informed of the progress of the team.

- Providing oversight of the content and distribution of all internal and external communications about the incident.
- Documenting all activities.

Containment

As the ISIRT begins conducting its investigation of a potential security breach, the containment phase must also commence. The goal of containment is to limit the extent of the incident and prevent the inundation of resources or broadening the damage, with an emphasis on maintaining or restoring business continuity. An incident is contained when no more harm is possible and the focus pivots to the remediation phase. The containment phase may focus on both short-term and long-term containment.

Requirements and considerations during the Containment phase include:

- Documenting all steps.
- Conducting a risk assessment of the incident.
  - Identify number of customers affected.
  - Identify type of breach/attack.
  - Determine how to prioritize identifying the attacker versus continuing or re-establishing business continuity.
  - Identify which systems are damaged or infected by malicious intrusions, if applicable.
  - Identify the exact type of data breach.
  - Interview all personnel involved with the incident.
  - Estimate the projected costs to repair the damage from the organization's perspective and, importantly, the customer's perspective.
  - Create a complete list of compromised accounts.
  - Decide whether to monitor, freeze or close affected accounts, if applicable.
  - Block and reissue credit cards, if needed.
  - Monitor and study affected accounts.
  - Determine fraud patterns.
  - Review/analyze all available logs.
  - Evaluate and respond to potential attack vectors and protect the network from their expansion.

Depending on the nature of the incident, institutions may consider:

- Shutting down affected systems.
- Disconnecting systems from the network.
- Disabling the network.
- Disabling services such as FTP, telnet, e-mail, or any other service that may be affected or may propagate the attack or breach.
- Stopping the attack from more damage by shutting off the power, pulling network cables, or blocking ports.
- Isolating affected systems from other resources.
- Conducting forensics and evidence preservation (e.g., memory dumps, drive images).
- Preserving and handling evidence according to established procedures to maximize successful prosecution of the perpetrator(s).

- Keeping detailed documentation of all evidence including information about personnel who handle evidence or information, time and date of handling, locations where evidence is stored, and security procedures for each step of evidence maintenance.

Eradication

The primary goal during the eradication phase of incident response is to remove any remaining trace(s) of the infection or cause from all network resources after having preserved any evidence needed for prosecution of the perpetrator(s). Once an incident has been isolated and contained, institutions should pursue an eradication strategy. It is important that institutions examine and eradicate all traces of the attack or breach in case a perpetrator left behind malware or logic bombs to reactivate an attack or breach after being reconnected to internal or external networks.

Examples of eradication steps include:

- Deleting infected files.
- Removing malware, such as Trojans and root kits.
- Disabling compromised accounts.
- Deleting fraudulent accounts.
- Blocking vulnerable application ports.
- Restoring compromised/corrupted operating system files.
- Replacing physical data drives.
- Performing a complete system reinstall.
- Changing host names, DNS entries or IP addresses.

It may also be practical during the eradication phase to install security controls and surveillance to prevent similar future attacks and improve physical security of equipment.

Remediation/Recovery

This phase ensures that the system returns to a fully operational status. It’s possible, even likely, that some of these steps may be addressed during the eradication phase. The type and scope of the security incident will dictate the recovery steps. Response teams need to determine whether to restore a compromised system or to rebuild the system or systems entirely. This will rely on presumably credible backups. Teams must make every effort to ensure restoration of system data. An incident could potentially corrupt data for many months before discovery. Therefore, it is very important that as part of the incident response process, institutions determine the duration of the incident.

Examples of remediation/recovery steps include:

- Rebuilding a “clean” system, while the compromised system is still functioning in order to maintain business continuity.
- Re-imaging infected systems.
- Performing a complete system reinstall.
- Improving physical security of equipment.
- Installing surveillance equipment.

Post-Incident Activities and Lessons Learned

At the conclusion of its full investigation and assessment, ISIRT shall prepare a report detailing the incident, the ensuing investigation, the response, and lessons learned. Key participants may also hold a wrap-up meeting to evaluate the incident and the incident handling policy and procedures.

If it is determined that a security breach has occurred and that the misuse of personal information has occurred, or is reasonably likely to occur, an institution shall make the required notifications set forth in KRS 61.933 (see attached). While not required by law, as a best practice if an initial notification of security breach has been made to commissioner of the Kentucky State Police, the Auditor of Public Accounts, the Attorney General and CPE and it is determined that a security breach did not occur and misuse of personal information did not, or is likely to not, occur, an institution should provide follow up notification to those agencies.

<u>Nonaffiliated Third Parties</u>

In accordance with KRS 61.932(b)1. and 2., a nonaffiliated third party that is provided access to personal information by an institution, or that collects and maintains personal information on behalf of an agency shall notify the agency in the most expedient time possible and within seventy-two (72) hours of determination of a security breach relating to the personal information in the possession of the nonaffiliated third party. The notice to the agency shall include all information the nonaffiliated third party has with regard to the security breach at the time of notification. Notice may be delayed if law enforcement notifies the nonaffiliated third party that the notification will impede a criminal investigation or would jeopardize national or homeland security. If notice is so delayed, notification shall be given by the nonaffiliated third party to the agency as soon as reasonably feasible.

In accordance with KRS 61.932(2)(a), agreements executed or amended on or after January 1, 2015, with a nonaffiliated third party resulting in the disclosure of personal information to the nonaffiliated third party shall include the following:

- A requirement that the nonaffiliated third party implement, maintain and update security and breach investigation procedures that are appropriate to the nature of the information disclosed, that are at least as stringent as the security and breach investigation procedures and practices maintained by the institutions and are reasonably designed to protect the personal information from unauthorized access, use, modification, disclosure, manipulation, or destruction.
- Specifications on how the cost of the notification and investigation requirements under KRS 61.933 are to be apportioned when a security breach is suffered by the agency or nonaffiliated third party.