Eastern Kentucky University
Policy and Regulation Library

11.2.3
Volume 11, Information Management
Chapter 2, Technologies
Section 3, Information Security Incident Response
Approval Authority: President
Responsible Executive: Chief Information Officer
Responsible Office(s): Information Technology
Effective: October 2, 2015 Issued: December 16, 2014
Last Revised: Next Review: Fall 2020

Information Security Incident Response

Regulation Statement

Eastern Kentucky University understands the importance and value of securing Personal Information and ensuring the appropriate confidentiality, integrity, and availability of the data.

This regulation establishes how Eastern Kentucky University will respond in the event of a Security Breach, in compliance with KRS 61.931 to 61.934, as well as an Information Security Incident. This regulation outlines an action plan that will be used to investigate a potential Security Breach or Information Security Incident, mitigate damage if a Security Breach occurs, and properly notify officials and Impacted Individuals.

Entities Affected by the Regulation

All University Community Members including all faculty, staff, and students as well as anyone doing business for or with the University.

Background

Effective January 1, 2015, per KRS 61.932, any agency or Non-Affiliated Third Party 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. This regulation codifies the University's compliance with KRS 61.931 to 61.934 by establishing reasonable investigation procedures and notification requirements in the event of a Security Breach and establishes reasonable investigation procedures for Information Security Incidents.

Procedures

INVESTIGATIVE PROCEDURE

1. Initial Investigation

When an Information Security Incident is reported, the Security Analyst and/or his or her representative(s), shall conduct an initial investigation to determine if an Information Security Incident has occurred. As part of the investigation, 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 investigation should be brief, but substantive enough to determine if an Information Security Incident has occurred. Some of the information to be gathered should be:

- When (date and time) did the incident occur?
- How did the incident happen?
- What type of data or information was exposed? (Detailed as possible)
- What group or number of people are affected?

(a) If an Information Security Incident has NOT occurred:

If after the initial investigation it is determined that an Information Security Incident has not occurred, the Security Analyst or his or her representative(s) shall document both the event and his or her investigative efforts, and close the matter. All documentation will be preserved pursuant to record retention schedules. In the event of misplaced or stolen EKU issued ID Cards, they will not be considered a Security Breach based on the protections in place.

(b) If an Information Security Incident has occurred:

If it is determined after the initial investigation that an Information Security Incident has occurred, an EKU Computing Emergency Response Team (ECERT) will be activated to begin a prompt and reasonable full investigation.

Duties of the ECERT shall include, as applicable:

- Identifying the individuals affected by the Information Security Incident/Security 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 the incident, which may include interviewing relevant individuals to learn the circumstances surrounding the incident and reviewing logs or other resources.
- If necessary, identifying and engaging consultants, as required to assist EKU in its investigation and/or risk analysis.
- Conducting a root cause analysis of the Information Security Incident/Security Breach.
- If a Security Breach has occurred, refer to the section, "PROCEDURES FOR NOTIFICATION IN THE EVENT OF A SECURITY BREACH".
- 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.
- 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.

2. Containment

As the ECERT begins conducting its investigation of a potential Information Security Incident/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 Impacted Individual's perspective.
- Create a complete list of compromised accounts.
- Decide whether to monitor, freeze, or close affected accounts, if applicable.
- Block and reissue Colonel 1 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, EKU will 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.
- Stopping the attack form more damage by shutting of 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 attacker(s).
- Keeping detailed documentation of all evidence including information about personnel who handle evidence or information, time and date of handling, locations where evidence stored, and security procedures for each step of evidence maintenance.

3. Eradication

The primary goal during the eradication phase of the incident response is to remove any evidence of the Information Security Incident/Security Breach from all network resources. Once an incident has been isolated and contained, EKU will pursue an eradication strategy to remove all traces of an attack. It is important that EKU examine and eradicate all traces of the attack in case an attacker left behind malware or logic bombs to reactivate an attack 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.
- Improving physical security of equipment.
- Installing surveillance equipment.
- Changing host names, DNS entries or IP addresses.

It may also be practical during the eradication phase to install security controls to prevent similar future attacks.

4. Remediation/Recovery

This phase ensures that the system returns to a fully operational status. The type and scope of the Information Security Incident/Security Breach will dictate the recovery steps. ECERT needs to determine whether to restore a compromised system or to rebuild the system or systems entirely. This will rely on presumably credible backups. ECERT must make every effort to ensure restoration of system data. An incident could potentially corrupt data for many months before discovery. Therefore, it will be very important that as part of the incident response process, ECERT determines the duration of the incident.

Examples of remediation/recovery steps include:

- Rebuilding a "clean" system, while 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.

5. Post-Incident Activities and Lessons Learned

At the conclusion of its full investigation and assessment, ECERT shall prepare a report detailing the incident, the ensuing investigation, the response, and lessons learned. Key participants may hold a wrap-up meeting to evaluate the Information Security Incident/Security Breach and the incident handling policy and procedure.

PROCEDURES FOR NOTIFICATION IN THE EVENT OF A SECURITY BREACH

Process for initial notification of a Security Breach:

If the Information Security Incident is determined to be a Security Breach, per KRS 61.933 (1) (a) (1), EKU shall notify as soon as possible but within seventy-two (72) hours of determination of the Security Breach the following officials:

- Commissioner of the Kentucky State Police
- Auditor of Public Accounts
- Attorney General
- President of the Council on Postsecondary Education

Process for additional notification upon determination that misuse of personal information has occurred or is likely to occur:

If it is determined that the misuse of Personal Information has occurred or is reasonably likely to occur:

- EKU shall notify in writing all officials listed above (KRS 61.933 (1) (a) (1)) and the Commissioner of the Department for Libraries and Archives within forty-eight (48) hours of the completion of the investigation;
- EKU shall notify all the Impacted Individuals impacted by the Security Breach within thirty-five (35) days of providing notifications of misuse to the officials listed above (KRS 61.933 (1) (a) (1)) and
- If the number of Impacted Individuals to be notified exceeds one-thousand (1,000), then EKU shall notify, at least seven (7) days prior to providing notice to those Impacted Individuals , the Council on Postsecondary Education and all consumer credit reporting agencies included on the list maintained by the Office of the Attorney General (KRS 61.933 (1) (b) (a-c)).

Process for additional notification upon determination that misuse of personal information has NOT occurred or is NOT likely to occur:

If EKU determines that the misuse of Personal Information has not occurred and is not likely to occur, EKU will notify the following that the misuse of Personal Information has not occurred:

- Commissioner of the Kentucky State Police
- Auditor of Public Accounts
- Attorney General
- President of the Council on Postsecondary Education

No other notifications will be required, but EKU is required to maintain records that reflect the basis for its decision for a retention period set by the State Archives and Records Commission as established by KRS 171.420 (KRS 61.933 (1) (b) (2)).

Requirements for providing notice to impacted individuals:

No notifications shall be made**:**

- If, after the consultation with a law enforcement agency, EKU receives a written request from a law enforcement agency for a delay of the notification because the notice may impede a criminal investigation. This may apply to some or all required notifications (KRS 61.933 (3) (a)).
- If EKU determines that measures necessary to restore the reasonable integrity of the data system to meet the notification timeframe cannot be implemented within the timeframe established by KRS 61.933 (1) (b) 1.b., and the delay is approved in writing by the Office of the Attorney General. If notice is delayed, notice shall be made immediately after actions necessary to restore the integrity of the data system have been completed.

Notice shall be provided by as follows:

- Conspicuous posting of the notice on EKU's website;
- Notification to regional or local media if the Security Breach is localized, and also to major statewide media if the Security Breach is widespread, including broadcast media, such as radio or television; and
- Personal communication to individuals whose data has been breached using one of the methods below that EKU believes is most likely to result in actual notification to those individuals, if EKU has the information available:
    - In writing, sent to the most recent address for the individual as reflected in EKU's records; or
    - By electronic mail, sent to the most recent electronic mail address for the individual as reflected in EKU's records, unless the individual has communicated to EKU in writing that they do not want email notification; or
    - By telephone, to the most recent telephone number for the individual as reflected in EKU's records (KRS 61.933 (2) (a) (1-3))

Information to be included in the clear and conspicuous notification:

The notification shall include:

- To the extent possible, a description of the categories of information that were subject to the Security Breach, including the elements of Personal Information that were or were believed to be acquired.

- Contact information for EKU, including the address, telephone number, and toll-free number if a toll-free number is maintained.
- A description of the general acts taken by EKU, excluding disclosure of defenses used for the protection of information, to protect the Personal Information from further Security Breach.
- The toll-free numbers, addresses, and Web site addresses, along with a statement that the individual can obtain information from the following sources about steps the individual may take to avoid identity theft, for:
    - The major consumer credit reporting agencies;
    - The Federal Trade Commission; and
    - The Office of the Kentucky Attorney General (KRS 61.933 (2) (b) (1-4).

NOTIFICATION PROCEDURES BASED UPON COMPLIANCE ISSUES

If a federal or state law or regulation requires notification of a Security Breach to Impacted Individuals, the University will follow the specific guidelines of the applicable federal or state law or regulation.

NONAFFILIATED THIRD PARTY CONTRACT REQUIREMENTS

Contract Requirements

For any agreements executed or amended on or after January 1, 2015, when EKU contracts with a Nonaffiliated Third Party and that discloses Personal Information to the nonaffiliated third party EKU shall require as part of that agreement 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 in accordance with policies established by the Council on Postsecondary Education, and that are reasonably designed to protect the personal information from unauthorized access, use, modification, disclosure, manipulation, or destruction (KRS 61.932 (2) (a)).

These agreements will be reviewed for approval by EKU's IT Security Analyst or designee for compliance to this Regulation.

Requirements for providing notifications and/or reports to EKU

A Nonaffiliated Third Party that is provided access to Personal Information by EKU, or that collects and maintains Personal Information on behalf of EKU shall notify EKU in the most expedient time possible and without unreasonable delay but 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 EKU shall include all information the Nonaffiliated Third Party has with regard to the Security Breach at the time of notification. Agreements shall specify how the cost of the notification and investigation requirements under KRS 61.933 are to be apportioned when a Security Breach is suffered by EKU or the Nonaffiliated Third Party (KRS 61.932 (2) (b) (1).

The notification to EKU may be delayed if a law enforcement agency notifies the Nonaffiliated Third Party that notification will impede a criminal investigation or jeopardize homeland or national security. If notice is delayed, notification shall be given as soon as reasonably feasible by the Nonaffiliated Third Party to EKU. EKU shall then record the notification in writing on a form developed by the Commonwealth Office of Technology that the notification will not impede a criminal investigation and will not jeopardize homeland or national security. The Commonwealth Office of Technology shall promulgate administrative regulations under KRS 61.931 to 61.934 regarding the content of the form (KRS 61.932 (2) (b) (2)).

If a Nonaffiliated Third Party is required by federal law or regulation to conduct Security Breach investigations or to make notifications of Security Breaches, or both, as a result of the Nonaffiliated Third Party's unauthorized disclosure of one (1) or more data elements of Personal Information, the Nonaffiliated Third Party shall meet the requirements of KRS 61.931 to 61.934 by providing to EKU a copy of any and all reports and investigations relating to such Security Breach investigations or notifications that are required to be made by federal law or regulations. This shall not apply if the Security Breach includes the unauthorized disclosure of data elements of Personal Information that are not covered by federal law or regulation but are listed in KRS 61.931 (6) (a) to (f). (KRS 61.932 (1) (c) (2)).

Definitions

- **ECERT:** EKU Computing Emergency Response Team. Members included but are not limited to:
    - Chief Information Officer or designee
    - Director of Infrastructure and Enterprise Systems
    - Director of Information Services
    - University Counsel
    - Security Analyst
    - Senior Network Engineer
- **FERPA:** Family Educational Rights and Privacy Act
- **GLB:** Gramm-Leach-Bliley Act- Related to the use of student financial aid and loans.

- **HIPAA:** Health Insurance Portability and Accountability Act
- **ID Card:** In the event of misplaced or stolen student/employee ID Card, it is the card holder's responsibility to promptly notify EKU's Card Services. Even though the ID contains Personal Information in the form of the card holder's name and picture with an EKU issued ID number, EKU will not determine this to be a Security Breach due to the following reasons:
    - In order for the ID number to be used to access any Personal Information of the card holder, a twelve (12) or more character password must be used.
    - The Code of Ethics for Computing & Communications specifically prohibits the sharing of a password.
    - Once Card Services is notified of the misplaced or stolen ID Card, the ID Card will be deactivated and cardholder will be reissued a new ID Card.
    - Once Card Services is notified of the misplaced or stolen ID Card, all account activity with the ID number will be monitored for a minimum of two (2) weeks with additional monitoring as needed.
    - Appropriate security protocols are in place for reissuing a password so that the cardholder can utilize his/her ID number. If a password must be reset, the following protocols must occur:
        - The cardholder can access their account by answering pre-determined security questions and reset their password.
        - The student cardholder can contact the Registrar's office and present photo identification in person and receive assistance in resetting the password.
        - The employee cardholder can contact the Human Resource's office and present photo identification in person or answer specific identifying questions over the telephone and receive assistance in resetting the password.
- **Impacted Individuals:** Individuals whose Personal Information has been compromised or reasonably may have which been compromised resulted in the likelihood of harm to the Impacted Individual.
- **Information Security Incident:** Any real or suspected event, accidental or intentional, which may compromise the security of Personal Information These include but are not limited to:
    - Attempts (either failed or successful) to gain unauthorized access to Personal Information.
    - 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.
    - The unauthorized or inappropriate use of a system or device for the viewing, transmitting, processing or storing of data.
    - Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

- **Nonaffiliated Third Party:** Any person that has a contract or agreement with EKU; and receives personal information from EKU pursuant to the contract or agreement (KRS 61.931(5) (a-b).
- **PCI-DSS:** Payment Card Industry Data Security Standards
- **Personal Information:** 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
    - 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;
    - A Social Security Number;
    - A taxpayer identification number that incorporates a Social Security number;
    - A driver's license number, state identification card number, or other individual identification number issued by any agency;
    - A passport number or other identification number issued by the United States government; or
    - 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 61.931 (6) (a-f))
- **Security Breach:** The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises or EKU 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 the unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted 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. (KRS 61.931 (9) (a))

Responsibilities

- Director of Creative Services or designee
    - Responsible for notification on EKU's website
- ECERT
    - Responsible for conduct investigation which consists of, but not limited to initial investigation risk assessment, determination of a Security Breach, and mitigation

- Human Resources
    - Responsible for notification to Faculty and Staff
- Registrar's Office
    - Responsible for notification to Students
- University Counsel or designee
    - Responsible for providing notifications pursuant to KRS 61.933 which includes the initial notification and additional notification upon identification that misuse of Personal Information has/has not occurred or is/is not likely to occur. Responsible for notification to appropriate federal or state agencies based upon applicable federal or state law or regulation. Responsible for ensuring that agreements between EKU and Nonaffiliated Third Parties contain appropriate data security measures, Security Breach investigation procedures, and notification requirements to Impacted Individuals.
- Vice President for Marketing and Communication
    - Responsible for notification to regional or local media

Interpreting Authority

Chief Information Officer

Statutory or Regulatory References

KRS 61.931 – 61.934

Relevant Links

- Family Education Rights and Privacy Act
- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act
- Payment Card Industry Data Security Standards

Regulation Adoption Review and Approval

Regulation Revised

Date	Entity	Action
October 2, 2015	President Michael T. Benson	Adopted

March 25, 2015	Provost Council	Approved
February 23, 2015	Staff Council	Approved

Regulation Issued

Date	Entity	Action
December 16, 2014	President Michael T. Benson	Adopted Interim