KENTUCKY STATE UNIVERSITY

Policies and Regulations

PROCEDURE TITLE: SECURITY INCIDENT RESPONSE

APPLIES TO:

All KSU students, faculty, staff, Board of Regent members, and all others who use, have access to, store, transmit or oversee KSU information technology resources. This applies to access of any KSU information resource from any device.

ADMINISTRATIVE AUTHORITY:

APPROVED BY: **Kentucky State University Board of Regents**

EFFECTIVE DATE: **August 8, 2025**

NEXT REVIEW DATE: **August 8, 2028**

PROCEDURE STATEMENT:

The purpose of this policy is to establish the appropriate response to identify, investigate, contain, eradicate, and remedy a security incident. The policy will also provide procedures to document, report and communicate the incident. Responsibility for each step will be established in this policy.

DEFINITIONS:

Confidential Data: This classification applies to the most sensitive data or information that is intended for use strictly within KSU, protected by any confidentiality agreements, or data protected by federal or state law, such as FERPA, HIPPA, GLBA or PCI-DSS. Its unauthorized disclosure could seriously and adversely impact KSU, its customers, its business partners, and its suppliers.

Restricted Data: This classification applies to less-sensitive business data or information that is intended for use within KSU. By default, all information that is not defined as confidential or public should be treated as restricted. Its unauthorized disclosure could adversely impact KSU, or its customers, suppliers, business partners, or employees, but would not violate law.

Information Security Incident: An actual or suspected event such as a violation of computer security policies, acceptable use policies, or standard security practices. These events may adversely affect the security of KSU's information resources or systems. Examples include:

- Web site defacement
- Theft or loss of a computing device that may contain PII whether or not such device is owned by KSU
- Unauthorized access to data, especially confidential data like a person's name and social security number
- Computer infected with malware such as a worm, virus, Trojan Horse, or botnet
- Reconnaissance activities such as scanning the network for security vulnerabilities
- Data Breach
- Misuse of Information Resources or Systems
- Denial of Service attack
- Security weakness such as an un-patched vulnerability

Personal Identifiable Information (PII): Per KRS 365.732 this is defined as individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted:

- Social Security number;
- Driver's license number; or
- Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account.

Information Technology Security Incident Response Team: – Members vary depending upon nature of the incident. Should contain at a minimum, General Counsel, CIO and Public relations. May include other individuals as needed such as the senior administrator for the affected unit, a representative from the police department, or director from human resources.

PROCESS:

Reporting Security Incidents:

1. Any member of the KSU community who suspects or becomes aware of an Information Security Incident must report the incident immediately by:

2. Contacting the IT Help Desk or Chief Information Officer by phone (preferred), e-mail or in person.

3. Contacting the department supervisor, who must contact the CIO immediately.

4. If the department supervisor is not available, then the individual must contact the division Vice President, who must contact the CIO immediately.

Responding to Incidents:

Once reported, the Chief Information Officer and General Counsel will conduct an initial investigation to determine if an information security incident has occurred by reviewing the type, scope and impact of the incident (see Appendix A). Based on the findings, one of the following processes will take place:

1. If it has been determined that an information security incident has not occurred, the event will be documented and closed.

2. If it has been determined that an information security incident has occurred and restricted or confidential data/information has been impacted, on a per incident basis, the creation of an Information Technology Security Incident Response Team (IT-SIRT), will be created to further investigate the incident. The incident will be

prioritized as high or critical and IT-SIRT will take necessary actions including but not limited to:

1. Detection and Analysis

   Key Functions:
   a. Following impact analysis
   b. Determining systems impacted
   c. Determining the exact type of incident.

2. Communication

   Key Functions:
   a. Determine appropriate notification requirements.
   b. If required, complete determined breach notification form in Appendix C.
   c. Develop an action plan for meeting notification requirements.

3. Containment

   Key functions:
   a. Stop potential loss of data.
   b. Prevent further damage or comprised systems and/or information.
   c. Protect other Information systems or resources.
   d. Identify the location and owner of the device in order to engage in containment, eradication, and recovery.
   e. Determine if delayed containment is necessary to collect evidence.
   f. Maximize the preservation of evidence.

4. Preservation of Evidence

   Key Functions:
   a. Make backups (preferably disk image backups, not file system backups) of affected systems.
   b. Make copies of log files that contain evidence related to the incident.
   c. Preserve evidence not already preserved.
   d. Perform additional evidence gathering activities.

5. Eradication

   Key Functions:
   a. Identify and mitigate all vulnerabilities that were exploited.
   a. Remove all traces of the attack or the breach.

6. Remediation

   Key functions:
   a. Return affected system to an operationally ready state.
   b. Ensure system returns to fully operational status.
   c. Improve physical security of equipment.

7. Documentation

   Key Functions:

   a. Create and issue final reports.

    b. Archive evidence and documentation.

8. Identify post-incident activities needed
    a. Determine lessons learned and make recommendations to prevent subsequent similar incidents
    b. Close out the incident

3. If it has been determined that an information security incident has occurred and restricted or confidential data/information has *not* been impacted, the CIO under the guidance of Legal Counsel will determine steps to communicate, contain, eradicate, remediate, document and as well determine any post-incident activities.

KSU will adhere to federal, state laws, rules, regulations, policies and procedures governing the confidentiality of data and notification of security breaches.

REFERENCES AND RELATED MATERIALS:

Appendix A: Security Incident Reporting Form

Date Submitted:_________/________/________

1. Reported By Contact Information	
Full Name:	
Job Title:	
Department/College:	
Office Room Number:	
Work Phone Number:	
Cellphone Number:	
Email Address:	
Additional Contact Information:	

2. **Type of Incident (Check all that apply)**

☐ Compromised/Stolen/Altered Data
☐ Theft and use of Others ID’s
☐ Denial of Service
☐ Unauthorized Access
☐ Data Breach
☐ Social Engineering (e.g. Phishing, scams)
☐ Website Defacement or Redirection
☐ Reconnaissance (e.g. scans, probes)
☐ Malicious Code (e.g. worms, virus, Trojan)
☐ Computing Device Lost, Stolen or Damaged
☐ Violation of Security Policy or Policies
☐ Other or Unknown (Provide description below)

Description of Incident:

3. Scope of Incident (Check all that apply)

- □ Critical (e.g. KSU is no longer able to provide some critical services to any user).
- □ High (e.g. KSU has lost the ability to provide critical service to a subset of system users).
- □ Medium (e.g. KSU can still provide critical services to all users and has lost no efficiency).
- □ Low (e.g. No effect to the organization’s ability to provide services to all users. Individual impact)
- □ Unknown (Provide description below)

Estimated number of systems impacted:	
Estimated number of users impacted:	
Impact on Third Parties? If so list.	

Additional scope information:

4. Impact Categories (Check all that apply)

- □ Loss of Access to Services
- □ Loss of Productivity
- □ Loss of Reputation or Integrity
- □ Loss of Revenue
- □ Propagation to other networks
- □ Unauthorized disclosure of data/information
- □ Unauthorized modification of data/information
- □ Other or Unknown (Provide description below)

Estimated total Cost:	

Additional Impact Information:

5. Affected Data (Check all that apply)

- □ Restricted or Confidential data/information
- □ Public data/information
- □ Financial data/information
- □ FERPA related data/information
- □ Personally Identifiable Information (PII)
- □ Intellectual Property/Copyrighted data/information
- □ Critical Infrastructure
- □ Other or Unknown (Provide description below)

Quantity of Data/Information impacted:	

Additional Affected Data/Information:

6. Analysis

Attack Sources (e.g. IP address, port)	
IP address of affected system	
Physical Location of Affected System:	
Additional Analysis Information:	

7. Timeline

Date and time when first detected, discovered or reported:	
Date and time when the incident first occurred:	
Date and time when the incident was contained or services restored:	
Date and time when Commonwealth “Determination of Breach Completed and Submitted”(If applicable)	
Date and time when Affected Users Notified (If applicable)	
Detailed incident timeline:	

8. Remediation and Post – Incident Summary

Actions Taken to Identify Affected Resources or Systems	
Actions Taken to Remediate Incident	
Actions Taken to Prevent Future Incidents	
Does existing administrative controls need to be amended?	

Was the response appropriate?	
What lessons have been learned from the incident?	
Should any Security Policies be updated?	
Additional Comments:	

Appendix B: Incident Handling Checklist

	Action	Completed
Detection and Analysis		
1	Determine whether an incident has occurred	
1.1	Review Impact Categories	
1.2	Determine if Restricted or Confidential Info was breached	
1.3	Determine Systems Impacted	
Communication		
2	Determine appropriate notification requirements.	
3	Develop an action plan for meeting notification requirements	
Containment, Eradication, Preservation of Evidence		
4	Acquire, preserve, secure and document evidence	
5	Contain the incident	
5.1	Stop potential loss of data	
5.2	Prevent further damage of compromised system and/or info	
6	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove all traces of the attack (Malware, inappropriate materials and/or other components)	
Remediate the Incident		
7	Return affected system to an operationally ready state	
8	Confirm that the affected systems are functioning normally	
Documentation		
9	Create and issue final reports.	
10	Archive evidence and documentation.	
Post-Incident Activities		
11	Determine lessons learned.	
12	Make recommendations to prevent subsequent similar incidents.	
13	Close out the incident.	

Appendix C: Determined Breach Notification Form (Commonwealth Form FAC-001)

Determined Breach Notification Form

Section 1

Complete and submit within 72 hours of determination or notification.

Determined

□ Finance Cabinet Secretary
□ Auditor of Public Accounts (APA)
□ Kentucky State Police (KSP)
□ Attorney General (AG)
□ Commissioner of Department of Library and Archives, if breach determined
□ Chief Information Officer of Commonwealth Office of Technology
If Department of Local Government under KRS 61.931(1)(b) or (c) also contact:
□ Commissioner of Department of Local Government
If Public School District listed in KRS 61.931(1)(d) also contact:
□ Commissioner of Kentucky Department of Education
If Educational entity listed under KRS 61.931(1)(e) also contact:
□ President of Council on Postsecondary Education

Agency Name: ______________________________

Agency Contact: ______________________________

Agency Contact Email: ______________________________

Agency Contact Phone Number: ______________________________

Date of Notification to Agencies: ____________________ Time of Notification: ____________

Date Breach Determined: ____________

Section 2

Complete this portion after the conclusion of the investigation regarding whether the Security Breach has resulted in or is likely to result in the misuse of personal information. Provide notice to agencies within 48 hours of completing investigation.

Personal Information Breached: □ Yes □ No

If Yes, Explain: ______________________________

Total Number of Individuals Impacted: ____________ Date Individuals Notified: ____________

Type of Notices Sent Out (select all that apply and provide explanations):

□ Web Posting: □ Email:

□ Local or Regional Media: □ Telephone:

□ Letter: □ Other:

Did You Notify Consumer Credit Reporting Agencies? □ Yes □ No If Yes, Date: ____________

Any Other Breach Compliance Requirements Apply such as Federal? □ Yes □ No

If Yes, Explain: ____________

Third Party Breach: □ Yes □ No

If Yes, Third Party Name: ____________

If Third Party Involved, When Did They Notify the Agency: ____________

If a delay then please attach the delay notification record along with supporting documentation. Was there a delay due to:

□ Law enforcement investigation. Reference to KRS 61.933 (3)(a)

□ An agency determines that measures necessary to restore the reasonable integrity of the data system cannot be implemented within the timeframe established and will delay the breach determination. Delay will need to be approved in writing from the Office of the Attorney General. Reference to KRS 61.933 (3)(b)

□

Section 3

Complete and submit at the conclusion of the investigation and any notice and resolution process.

Actions Taken to Resolve Breach:

____

Actions Taken to Prevent Additional Security Breaches in Future, if any:

____

A General Description of what Actions are Taken as a Matter of Course to Protect Personal Data from Security Breaches:

____

Any Quantifiable Financial Impact to the Agency Reporting the Security Breach:

____

KRS 61.931 to 61.934 - https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=43575
KRS 42.726 - https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=55894

REFERENCES AND RELATED MATERIALS:

- KSU Data Classification Policy
- KSU Data Security Controls Regulation
- KSU Data Access Management Regulation
- KSU Data Backup and Disaster Recovery Regulation

CONTACTS:

Subject	Office	Telephone	E-mail
General Questions	Office of the CIO	(502) 597-7000	Wendy.Dixie@kysu.edu

HISTORY:

Revision Type	Date of Issuance/Revision	Drafter(s)/Editor(s)
Issued (New Policy)	September 2019	Wendy Dixie
Revised (New Template and Substantive Revisions)	June 2025	Zach Atwell