Education and Workforce Development Cabinet
POLICY/PROCEDURE

Policy Number: EDU-00

Effective Date: 6/08/17
Review Date: 6/12/18
Revision Date:

Subject: Security Incident Handling Policy

Policy Statement: This policy identifies the necessity and procedures for EDU to identify and notify appropriate personnel when a security incident occurs. Timely identification and notification of incidents allow EDU to respond expeditiously to information security threats against Commonwealth resources.

Applicability: This policy shall be adhered to by all state and local entities and their users, including employees, contractors, consultants, temporaries, volunteers and other workers that connect to the Commonwealth's network and computing infrastructure.

Responsibility for Compliance: EDU is responsible for assuring that employees within their organizational authority are aware of the provisions of this policy, that compliance by the employee is expected and that attempts to forego compliance with this policy may result in disciplinary action pursuant to KRS 18A up to and including dismissal. Failure to comply may result in additional shared service charges to EDU for COT's efforts to remediate information security incidents resulting from non-compliance with this policy.

Review Cycle: This policy will be reviewed Annually.

Definitions:

- Information Security Incident: An information security incident, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the exploited weaknesses, and restoring computing services.

Policy: When EDU identifies or suspects a potential security incident or a breach or loss of personally identifiable information, including Social Security Administration provided information (SSPI) and Federally Transmitted Information (FTI), EDU OTS Security are required to contact the Commonwealth Service Desk (CommonwealthServiceDesk@ky.gov or (502) 564-7576) to report the incident. EDU OTS Security is required to notify the SSA contact with in one (1) hour and the IRS contact within twenty-four (24) hours of a potential Security Breach of their respective information.

All other incidents shall be handled in accordance with KRS 61.931-61.933, Personal Information Security and Breach Investigations and are to be reported within seventy-two (72) hours. In the event that the incident is sensitive in nature, OTS can contact the COT Security Office (COTSecurityOperations@ky.gov or 502-564-1532) directly instead of the Commonwealth Service Desk. These actions allow the Office of the CISO to review the incident and determine the level of required involvement with the incident response. Depending on

the scope of the incident and the skill set of the agency's personnel, COT's level of response may range from an advisory role to leading the investigation.

In any event, the CISO or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office of the SSA System Security Contact within one (1) hour of the experienced or suspected breach, loss or security incident, the responsible State Agency official or delegate must report the incident by contacting ***SSA's National Network Service Center (NNSC) toll free at 877-697-4489*** (select "Security and PII Reporting" from the option list). COT will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.

If SSA, or another Federal investigating entity (e.g. TIGTA or DOJ) determines that the risk presented by a breach or security incident requires that the state agency notify the subject individuals, the agency must agree to absorb all costs associated with notification and remedial actions connected to security breaches**. SSA and NIST Guidelines encourage agencies to consider establishing incident response teams to address PII and SSA-provided information breaches.**

Incident reporting policies and procedures are part of the security awareness program. Incident reporting pertains to all employees, or agents regardless as to whether they have direct responsibility for contacting SSA. The written policy and procedures document should include specific names titles or functions of the individuals responsible for each stage of the notification process. The document should include detailed instructions for how, and to whom each employee, contractor, or agent should report the potential breach or SSA-provided information (PII) loss.

The Office of the CISO will review all incidents and, on a case-by-case basis, determine whether to become actively involved depending on the actual or potential expansion of the incident to other assets or agencies. COT will maintain confidentiality on any issues as regulations and policies permit. EDU will work closely with COT to coordinate activities with appropriate entities to recover from security incidents.

EDU personnel will comply with all federal and state laws and policies for information disclosure to media or the public. EDU will work closely with the management of COT to ensure proper disclosure of security incident information. EDU personnel will not disclose agency data or information related to security incident responses unless required to do so by state or federal regulations.

Review Cycle:

Annually

Timeline:
Review Date: June 08, 2017
Reviewed By: EDU Agency Security Contacts

Enterprise Security and Policies
Cross Reference: http://technology.ky.gov/policy/Pages/CIO-090.aspx