SOWELA
TECHNICAL COMMUNITY COLLEGE
www.sowela.edu

**TITLE: Personal Information Security Breach Notification Policy**

**EFFECTIVE DATE: August 13, 2014**
**LAST REVISION:** **Policy No. 7012.1**

**Introduction**
The State of Louisiana Database Security Breach Notification Act (LA R.S. 51:3071), requires state agencies to notify persons whose "personal information" held by an agency has been compromised by a "security breach" as defined in the Act. This policy sets forth the circumstances and procedures under which required notifications will be made.

**Policy Statement**
Should a Database Security Breach occur within College's network, SOWELA Technical Community College will investigate and provide notice of information security breach to affected individuals in accordance with the State of Louisiana requirements as contain in LA R.S. 51:3071

**Definitions**
"**Personal information**" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:

a) Social Security Number.
b) Driver's license number.
c) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account(s).

"**Personal information**" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"**Breach of the security of the system**" means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person. Good faith acquisition of personal information by an employee or agent of an agency or person for the purposes of the agency or person is not a breach of the security of the system, provided that the personal information is not used for, or is subject to, unauthorized disclosure.

**Procedures in the Event of Any and All Breaches: Containment, Classification, and Report of a Breach.**

***Containment***
The first priority after any type of breach is discovered is to contain the breach and notify supervisory personnel as quickly as possible. The data must be secured, and the reasonable integrity, security, and confidentiality of the data or data system must be restored.

***Classification and Internal Reporting***
The next step is to determine the exact nature of the breach in terms of its extent and seriousness. The supervisor of the department where the breach occurred must take immediate action to determine the extent of the breach and to take such further action as is necessary to contain the breach or recover the missing data. Assistance from the College Information Technology Department, other office with relevant expertise should be requested as soon as possible. The supervisor must document the breach, the scope of the breach, steps taken to contain the breach, and the names or categories of persons whose personal information was, or may have been, accessed or acquired by an unauthorized person.

***Action Steps after Discovery of Any and All Breaches***
Contact the LCTCS Counsel and/or the SOWELA's Chief Information Resources and Technology Officer for guidance.

**Disclosure Upon Breach in the Security of Personal Information; Notification Requirements; Exemption**

A. Any person who conducts business in the state or who owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

B. Any agency or person that maintains computerized data that includes personal information that the agency or person does not own shall notify the owner or licensee of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of security of the system.

C. The notification required pursuant to Subsections A and B of this Section shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in Subsection D of this Section, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.

D. If a law enforcement agency determines that the notification required under this Section would impede a criminal investigation, such notification may be delayed until such law enforcement agency determines that the notification will no longer compromise such investigation.

E. Notification will be provided by one or more of the following methods:

1) Written notification.
2) Electronic notification, if the notification provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001.
3) Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed two hundred fifty thousand dollars, or that the affected class of persons to be notified exceeds five hundred thousand, or the agency or person does not have sufficient contact information. Substitute notification shall consist of all of the following:

   (i) E-mail notification when the agency or person has an e-mail address for the subject persons.
   (ii) Conspicuous posting of the notification on the Internet site of the agency or person, if an Internet site is maintained.
   (iii) Notification to major statewide media.

F. Notwithstanding Subsection E of this Section, an agency or person that maintains a notification procedure as part of its information security policy for the treatment of personal information which is otherwise consistent with the timing requirements of this Section shall be deemed to be in compliance with the notification requirements of this Section if the agency or person notifies subject persons in accordance with the policy and procedure in the event of a breach of security of the system.

G. Notification under this title is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.

**Reference**
LA R.S. 51:3071 et seq.
15 U.S. Code § 7001 - General rule of validity
U.S. Department of Education, Privacy Technical Assistance Center (PTAC): Data Breach Response Checklist, (September, 2012):
http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf

Source of Policy: Information Resources &Technology Division
Responsible: Administrator: Chief Information Resources & Technology Officer
Related Policy: N/A

LCTCS Policy Reference: N/A
LCTCS Guideline Reference: N/A

Approved by: _____ Chancellor

Date: 8/13/14