POLICY STATEMENT NO. 3 18.01

COORDINATED BY: Offices of Business Affairs/
Department of Computing Services

EFFECTIVE: June 7, 2006 REVISED: 1/2/08

SUBJECT: Database Security Breach Notification

I. PURPOSE

To state the campus policy on database security breach notification. Act No. 499 of the 2005 Regular Legislative Session enacted the Database Security Breach Notification Law. This policy provides the procedures for disclosure upon breach or the suspicion of breach in the security of LSUS employee, student and vendor personal information. Data covered by this policy may be in electronic or written form.

II. POLICY

1. Definition of terms:

   A. "Breach of the security of the system" means the compromise of the security, confidentiality, or integrity of computerized or written data that results in, or there is reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by the university, a university employee or a vendor.
   B. "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:
      1. Social security number.
      2. Driver's license number.
      3. 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.
      4. Personal information will be that of a current or former; student, employee or vendor of the university.

2. Data covered by this policy may be in written form or may reside electronically on traditional devices such as mainframes, servers and personal computers (desktop or laptop), on newer devices such as PDAs and cell phones or on state-of-the-art devices that may be developed. These devices may be University owned or may be owned by an employee or vendor.

3. Unauthorized access to the information described in this policy may be done electronically, via stolen equipment, or via unauthorized entry into buildings or rooms that enabled access to the information by unauthorized person(s).

4. Procedures to be followed upon the discovery of, or suspicion of, a breach in the security of

personal information:

A. Any employee who detects or has suspicion that personal information was released through a breach of data security must immediately notify the Director of Computing Services.
B. Any vendor that conducts business with LSUS or that owns or licenses computerized data that includes personal information, as described in this policy, following discovery or the suspicion of a breach in the security of the data, shall immediately notify the Director of Computing Services.
C. The Director of Computing Services will investigate the security problem to determine if there was a breach and to determine what information was obtained or may have been obtained by the unauthorized person(s). If it is determined that a breach has occurred, the Director of Computing Services will notify the Director of University Police. The Director of University Police may request other law enforcement agencies (i.e. Shreveport Police Department, FBI, etc) to assist in any investigation.
D. Upon completion of their investigation the Directors of Computing Services and University Police will notify the Vice Chancellor for Business Affairs of the results of the investigation and recommend appropriate action.

5. Employees who maintain personal information (as described above) obtained via the University or from a University related activity on their personal computers (desktop or laptop), on newer devices such as PDAs and cell phones or on state-of-the-art devices that may be developed must also follow this policy.

6. Departments who enter into contracts with vendors to maintain data off site that includes any personal information, as described above, must make this policy part of the contract with the vendor.

7. Notification to employees and students of the unauthorized release of personal information.

The Department of Computing Services, upon the approval of the Vice Chancellor for Business Affairs, shall notify any university employee or student whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.

If the University Police Department or other law enforcement agency determines that the notification required 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.

Notification of the unauthorized release of personal information will be done via one 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 U.S.C 7001.
3. Substitute notification if the cost of providing notification would exceed two hundred and fifty thousand dollars or if the number of persons in the affected class to be notified exceeds five hundred thousand or if LSUS does not have sufficient contact information. Substitute notification shall consist of all of the following:
   a. E-mail notification if an e-mail address is available.
   b. Conspicuous posting of notification on the LSUS Homepage.
   c. Notification to major statewide media.

4. Notification is not required if, after reasonable investigation, the Departments of Computing Services and University Police determine that there is no reasonable likelihood of harm to employees or students. The Vice Chancellor for Business Affairs must concur with this assessment.

AUTHORIZED:	Michael T. Ferrell Vice Chancellor for Business Affairs	1/2/08 Date
APPROVED:	Vincent J. Marsala Chancellor	1/2/08 Date