POLICY STATEMENT 6.20
SECURITY OF DATA

POLICY DIGEST

Monitoring Unit: Information Technology Services
Initially Issued: October 3, 2006
Last Revised: May 20, 2009

I. PURPOSE

This Policy Statement outlines the responsibilities of all users in supporting and upholding the security of data at Louisiana State University ("LSU" or the "University") regardless of user's affiliation or relation with the University, and irrespective of where the data is located, utilized, or accessed. All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of data from unauthorized generation, access, modification, disclosure, transmission, or destruction. Specifically, this Policy Statement establishes important guidelines and restrictions regarding any and all use of data at, for, or through Louisiana State University. This policy is not exhaustive of all user responsibilities, but is intended to outline certain specific responsibilities that each user acknowledges, accepts, and agrees to follow when using data provided at, for, by and/or through the University. Violations of this policy may lead to disciplinary action up to and including dismissal, expulsion, and/or legal action.

II. DEFINITIONS

For the purposes of this Policy Statement, the following definitions shall apply:

Computing resources: shall be defined as all devices (including, but not limited to, personal computers, laptops, PDAs and smart phones) owned by the University, the user or otherwise, which are part of or are used to access (1) the LSU network, peripherals, and related equipment and software; (2) data communications infrastructure, peripherals, and related equipment and software; (3) voice communications infrastructure, peripherals, and related equipment and software; (4) and all other associated tools, instruments, facilities, and the services that make use of any technology resources owned, operated, or controlled by the University. Computing resources or components thereof may be individually assigned or shared, single-user or multi-user, stand-alone or networked, and/or mobile or stationary.

Data: shall include all information that is used by or belongs to the University, or that is processed, stored, maintained, transmitted, copied on, or copied from University computing resources.

Data Steward(s): shall be defined as the functional unit(s) that is responsible for the collection, maintenance, and integrity of the data.

Functional unit(s): shall include any campus, college, program, service, department, office, operating division, vendor, facility user, or other person, entity or defined unit of Louisiana State University that has been authorized to access or use computing resources or data.

Least privilege: shall be defined as the principle that requires each person and/or functional unit be granted the most restrictive set of privileges needed for the performance of authorized tasks.

"Protected information: shall be defined as data that has been designated as private or confidential by law or by the University. Protected information includes, but is not limited to, employment records, medical records, student records, education records, personal financial records (or other personally identifiable information), research data, trade secrets, and classified government information. Protected information shall not include public records that by law must be made available to the general public. To the extent there is any uncertainty as to whether any data constitutes protected information, the data in question shall be treated as protected information until a determination is made by the University or proper legal authority.

User(s): shall be defined as any person or entity that utilizes computing resources, including, but not limited to, employees (faculty, staff, and student workers), students, agents, vendors, consultants, contractors, or sub-contractors of the University.

III. GENERAL POLICY

Louisiana State University functional units operating or utilizing computing resources are responsible for managing and maintaining the security of the data, computing resources and protected information. Functional units are responsible for implementing appropriate managerial, operations, physical, and technical controls for access to, use of, transmission of, and disposal of data in compliance with this policy. This requirement is especially important for those computing resources that support or host critical business functions or protected information.

Protected information will not be disclosed except as provided by University policy and procedures, or as required by operation of law or court order.

Any electronic data of the University shall be classified as public, private, or confidential according to the following categories:

A. *Public data:* Public data is defined as data that any person or entity either internal or external to the University can access. The disclosure, use, or destruction of public data should have no adverse effects on the University nor carry any liability (examples of public data include readily available news and information posted on the University's website).

B. *Private data:* Private data is any data that derives its value from not being publicly disclosed. It includes information that the University is under legal or contractual obligation to protect. The value of private data to the University and/or the custodian of such data would be destroyed or diminished if such data were improperly disclosed to others. Private data may be copied and distributed within the University only to authorized users. Private data disclosed to authorized, external users must be done in accord with a Non-Disclosure Agreement (examples of private data include employment data).

C. *Confidential data:* Confidential data is data that by law is not to be publicly disclosed. This designation is used for highly sensitive information whose access is restricted to authorized employees. The recipients of confidential data have an obligation not to reveal the contents to any individual unless that person has a valid need and authorized permission from the appropriate authority to access the data, and the person revealing such confidential data must have specific authority to do so. Confidential data must not be copied without authorization from the identified custodian (examples of confidential data include personally identifiable information

in student education records, and personally identifiable non-public information about University employees).

Please see Classification of Data for a general guide to determine which data classification is appropriate for a particular information or infrastructure system.

Although some protected information, private data, and confidential data the University maintains may ultimately be determined to be "public records" subject to public disclosure, such status as public records shall not determine how the University classifies and protects data until such a determination is made. Often public records are intermingled with confidential data and protected information, so all the information and data should be protected as confidential until it is necessary to segregate any public records.

It shall be the responsibility of the data steward(s) to classify the data, with input from appropriate university administrative units and legal counsel. However, all individuals accessing data are responsible for the protection of the data at the level determined by the data steward(s), or as mandated by law. Therefore, the data steward(s) are responsible for communicating the level of classification to individuals granted access. Any data not yet classified by the data steward(s) shall be deemed confidential. Access to data items may be further restricted by law, beyond the classification systems of Louisiana State University.

All data access must be authorized under the principle of least privilege, and based on minimal need. The application of this principle limits the damage that can result from accident, error, or unauthorized use. All permissions to access confidential data must be approved by an authorized individual, and written or electronic record of all permissions must be maintained.

Protected information shall not be provided to external parties or users without approval from the data steward. In cases where the data steward is not available, approval may be obtained by the Director or Department Head of the office in which the data is maintained, or by an official request from a senior executive officer of the University (i.e., President, Chancellor, Executive Vice Chancellor/Provost, or Vice Chancellor).

When an individual that has been granted access changes responsibilities or leaves employment, all of their access rights should be reevaluated and any access to protected data outside of the scope of their new position or status should be revoked.

Data that is critical to the mission of the University shall be located, or backed up, on centralized servers maintained by the institution, unless otherwise authorized by the data steward of that data, or Office of the Vice Chancellor for Information Technology (OVCIT).

In the interest of securing information protected under FERPA, GLBA, HIPAA, other state and federal legislation, University policies (e.g. PS-113: Social Security Number Policy), and reducing the risks to the University of fines and other penalties, all users of computing resources shall follow Best Practices for Confidential, Private, or Sensitive Data and Best Practices for Securing Systems.

NOTE: Please see Data Encryption for options to secure data.

IV. PROCEDURES

Complaints or concerns about violations of this or other technology policies should be sent to

security@lsu.edu. After verification is complete using system or other logs, and in accordance with other applicable policies and procedures, the incident will be reported to the appropriate Dean, Director, or Department Head for review and possible action.

V. SOURCES

PS-1 Equal Opportunity
PS-06.15 Use of Electronic Mail (E-mail) PS-06.25
Privacy of Computing Resources
PS-10 Internal and External Communications/Advertisements PS-30 Privacy
Rights of Students (Buckley Amendment)
PS-40 Employee Records Confidentiality PS-107
Computer Users' Responsibilities PS-113 Social
Security Number Policy PS-114 Security of Computing
Resources LSU Code of Student Conduct
PM-36 Louisiana State University System Information Security Plan The Louisiana
Database Security Breach Notification Law (Act 499)