POLICY STATEMENT 6.25
PRIVACY OF COMPUTING RESOURCES

POLICY DIGEST

Monitoring Unit: Information Technology Services
Initially Issued: October 3, 2008
Last Revised:

I. PURPOSE

Louisiana State University (LSU or the "University") is respectful of the privacy of authorized users of University computing resources and data. However, there are legitimate reasons for persons other than the account holder to access data, computing resources or network traffic, including, but not limited to, ensuring the continued integrity, availability, and confidentiality of University operations and systems; to secure user or system data; to ensure lawful and authorized use of University computing resources; and to respond to valid legal process or legal demands for access to computing resources and University records. This policy seeks to facilitate teaching, research, and the overall mission of the University through the authorized use of computing resources and data consistent with the University's need for limited access by persons other than the account holder when necessary to serve or protect operations within the University or to meet legal requirements. This policy applies to all authorized users of computing resources at LSU regardless of user's affiliation or relation with the University, and irrespective of where the resources are located, utilized, or accessed. Nothing in this policy is intended or shall be interpreted to waive, limit, or otherwise restrict the rights of the University to manage and allocate use of its computing resources and data or the responsibilities of Users under PS-06.15, PS-06.20, PS-101, PS-107, PS-114, or PM-36.

II. DEFINITIONS

For the purposes of this policy, the following definitions shall apply:

Authorized users: are people acting within the scope of a legitimate affiliation with the University, using their approved and assigned credentials and privileges, to gain approved access to University computing resources. A person acting outside of a legitimate affiliation with the University or outside the scope of their approved access to University computing resources is considered an unauthorized user.

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.

Content-neutral information: is information relating to the operation of systems, including information relating to interactions between individuals and those systems. Such information includes, but is not limited to, operating system logs (e.g., record of actions or events related to the operation of a device or system), user login records (e.g., logs of usernames used to connect to University systems, noting source and date/time), dial-up logs (e.g., connections to University modems, noting source, date/time, and caller id), network activity logs (e.g., connections attempted or completed to University systems, with source and date/time), non-content network traffic (e.g., source/destination IP address, port, and protocol), e-mail logs (e.g., logs of e-mail sent or received by individuals using University e-mail systems, noting sender, recipient, and date/time), account/system configuration information, and audit logs (e.g., records of actions taken on University systems, noting date/time).

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.

IT administrator/technician: is a person employed, contracted or assigned by LSU to maintain and operate a computer system or network or any portion thereof. The duties of an IT administrator/technician vary widely from one unit to another. IT administrators/technicians are usually charged with installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other problems.

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

Except in those circumstances in which access is appropriate to serve or protect operations within the University and to meet legal requirements as outlined in this policy, stored data, and voice and data network communications will not be accessed by information technology (IT) administrators/technicians or anyone other than:

A. the person to whom the account in which the data has been stored is assigned; or

B. the person from whom the communication originated, or to whomthe communication was sent; or

C. the person to whom the device containing the stored data has been assigned.

Although the University seeks to create an atmosphere of privacy with respect to its data and use of its computing resources, users should be aware that because LSU is a public institution, and because the University must be able to ensure the security, integrity and continuity of its operations, use of the University's computing resources cannot be completely private. For example, in addition to the types of permissible access described herein, e-mails sent or received through University e-mail accounts, may be subject to disclosure as public records in response to public records requests under Louisiana law. Further, documents including e-mails that are personally identifiable to a student may be education records of that student subject to inspection by that student under federal law. E-mails and other documents and data must be accessed by the University to make such determinations. Users should be aware that although the University will take reasonable measures to ensure the privacy of University computing resources as outlined in this policy, the University cannot guarantee absolute privacy as relates to any particular User.

IV. PROCEDURES

Except as provided herein, IT administrators/technicians at LSU may not access or facilitate access to the computer accounts or associated network traffic of someone other than the person to whom the personal computer account or computer is assigned. This includes data, voice and other files, including electronic mail (e-mail) and voicemail, encrypted on, stored on, or in transit to or from individual computer or voicemail accounts on University-owned devices/systems, personally-owned devices on University property (e.g., residence hall rooms) or devices/systems managed by the University on behalf of affiliated organizations (e.g., LSU Foundation or the LSU Alumni Association).

The exceptions to the above are as listed below:

A. An IT administrator/technician may access or permit access in the following cases:

1. Pursuant to authorization from the owner (the individual to whom the account or device or communication has been assigned or attributed);

2. To investigate potential violations of law or policy - with written authorization from Human Resource Management, or from the Office of the Dean of Students for situations where there is reasonable concern that the individual to whom the account or device is assigned or owned has engaged, is engaging, or imminently intends to engage, in illegal activities or violations of University policy using the account or device in question;

3. For critical operations - with written authorization from Human Resource Management, or the Office of the Dean of Students for situations in which retrieving the material is critical to the operation of the unit and when the account holder is deceased, terminated, incapacitated, unavailable, or unwilling to provide access;

4. On behalf of a deceased or incapacitated individual - with written authorization from Human Resource Management, or the Office of the Dean of Students to provide access to a lawful representative (e.g., spouse, parent, executor, holder of

power of attorney) of a deceased or incapacitated employee, faculty member, or student;

5. For internal audits - with written request from the Vice Chancellor of Finance and Administrative Services, or LSU System Office Director of Internal Audit for information relating to specific audits or investigations;

6. In response to legal process or demand - with written authorization from Human Resource Management, or the Office of the Vice Chancellor for Finance and Administrative Services confirming that access is required under the terms of a valid subpoena, court order, warrant, or other legal demand, or access is required under an applicable law, regulation, or University policy;

7. To minimize or mitigate substantial University risk – with written authorization from Human Resource Management, the Director of Public Safety, or the Office of the Dean of Students to address an emergency or to avoid or minimize exposure of the University to substantial risk of harm or liability;

8. For emergency problem resolution – when the IT administrator/technician has a reasonable concern that a program or process active in the account or on the device is causing or will cause significant system or network degradation, or could cause loss/damage to a system or other users' data. This includes forensic and/or other analysis in response to a security incident, sensitive data exposure, or system/device compromise;

9. To access system-generated, content-neutral information – for the purposes of analyzing system and storage utilization, problem troubleshooting, security administration, and in support of audits;

10. To investigate security incidents - The incident response function within the IT Security & Policy Office is responsible for investigating reports of abuse or misuse of University computing resources. Incident response staff may use system-generated, content-neutral information for the purposes of investigating technology misuse incidents, and in support of audits;

11. For routine monitoring of network communications - Security personnel in the IT Security & Policy Office and the Network Operations Center (NOC) may observe, capture, and analyze network communications. “Network communications” may contain content data and in some cases this content may be viewed during analysis. If any data must be stored to complete the assigned tasks, it will be stored securely and deleted as soon as possible;

12. Pursuant to implied consent – in situations where a user has requested assistance diagnosing and/or solving a technical problem or where the IT administrator/technician is performing required maintenance. In these cases, IT administrators/technicians shall limit the scope of the access to that which is necessary to address the problem or the task.

13. To protect University assets – when there is reasonable concern that the intellectual property, research, trade secrets, or other assets of the University are

in jeopardy, and pursuant to written authorization from Human Resource Management, the Vice Chancellor for Research, or the Vice Chancellor for Finance and Administrative Services.

B. Preservation of electronic information and of computing resources:

The copying and secure storage of the contents of an individual's e-mail, other computer accounts, office computer, or transient network traffic to prevent destruction and loss of information may occur:

1. Upon receiving credible notification of a University or law enforcement investigation for alleged illegal activity or violations of University policy on the part of a member of the University community; or

2. Upon receiving advice by the University's legal counsel that such copying and storage is otherwise needed in order to comply with legal obligations to preserve electronic information or secure computing resources; or

3. Upon receiving authorization from Human Resource Management, or LSU Police, or the Office of the Dean of Students indicating that such preservation reasonably appears necessary to protect University operations; or

4. When there is a reasonable concern that illegal activity or violations of University policy have occurred, are occurring, or are imminent, as determined by the Office of the Vice Chancellor for Information Technology (VCIT); or

5. As a routine backup procedure for disaster recovery or archival purposes.

Note: Access to such copies and stored materials shall be in accordance with this policy. Preserved materials that are no longer needed shall be destroyed in a secure manner.

Note for sections 4.1 and 4.2: IT administrators/technicians accessing computing resources covered by this policy shall 1) maintain the privacy of both the contents and the act of the access, except as otherwise required by this policy, or when necessary to report potential violations of law or University policy, and then only to the appropriate authority; and 2) make reasonable efforts to report such actions to the affected individual prior to that access, except when:

C. Prior notification is not appropriate or practical due to the urgency of the circumstances;

D. Such notice may result in destruction, removal, or alteration of data; or

E. Other circumstances make prior notice inappropriate or impractical.

Where prior notification is not appropriate or practical, reasonable efforts will be

made to notify the affected individual as soon as reasonable under the circumstances. No notification is necessary if access is for strictly routine backup, disaster recovery, or for archival purposes.

F. Other provisions:

1. Coordination with the Office of the Vice Chancellor for Information Technology (VCIT) – IT administrators/technicians receiving requests for access to computer accounts, files, or network traffic by persons other than the account holder shall consult with the VCIT prior to granting the access. The Chief IT Security & Policy Officer will ensure that the provisions of this policy have been followed. Where prior consultation is not possible, the IT administrator/technician shall notify the Chief IT Security and Policy Officer as soon as possible after the access has been granted.

2. Advice and interpretation - The Chief IT Security & Policy Officer in the VCIT represents the Vice Chancellor for Information Technology and CIO for these issues and is also available to provide advice and policy interpretation to department management and any member of the LSU community.

3. Legal requests - All legal requests or demands for access to computing resources or electronic information and all subpoenas, warrants, court orders, and other legal process, or demands directing that access be afforded to law enforcement agencies or others, must be delivered immediately to the Office of the Vice Chancellor for Finance and Administrative Services. Should such documents be served on individual, employees, or IT administrators/technicians, the documents must be sent immediately to the Office of the Vice Chancellor for Finance and Administrative Services for review. The Office of the Vice Chancellor for Finance and Administrative Services will review the request or order, and advise the relevant personnel on the necessary response. In the event that a law enforcement agency seeks to execute a search warrant or other order immediately and will not wait for review, individual IT administrators/technicians or other persons receiving such orders should not obstruct the execution of the warrant or order, but should document the actions by law enforcement, notify the Office of the Vice Chancellor for Finance and Administrative Services as soon as possible, and take reasonable steps whenever possible to preserve a copy of any data being removed, for appropriate University use.

4. Initiating access - Persons seeking access to specific computing resources and/or electronic information assigned to or associated with an individual, that are maintained by Information Technology Services (ITS), must send those requests to its-policy@lsu.edu . Acting for the Vice Chancellor for Information Technology and CIO, the Chief IT Security and Policy Officer will ensure adherence to proper policy and procedures and will coordinate any subsequent approved access. In addition, persons seeking access to specific computing resources and electronic information primarily assigned or associated with other persons, and that are not maintained by Information Technology Services (ITS), should direct those requests to the Chief IT Security and Policy Officer for approval.

Note: “Persons seeking access” include IT administrators/technicians who receive requests from others to access those resources or information. The Chief IT Security & Policy Officer is available to assist IT administrators/technicians with following proper policy and procedure.

V. SANCTIONS

Failure to comply with this policy and/or other LSU information technology policies may result in sanctions relating to: (a) the individual’s use of computing resources (such as suspension or termination of access, or removal of online material); (b) the individual’s employment (up to and including immediate termination of employment); (c) the individual's status as a student with the University (such as student discipline in accordance with applicable University policy); (d) civil or criminal liability; or (e) any combination of these.

VI. COMPLAINTS

Persons who have reason to believe that computer privacy has been violated should first contact the VCIT, in writing, describing the nature of the complaint. If the complaint is not resolved by the VCIT to the satisfaction of the User, employees may appeal to Human Resource Management and students may appeal, in writing, pursuant to PS-48. Others persons may appeal, in writing, to the Office of the Vice Chancellor for Finance and Administrative Services.

VII.SOURCE

PS-06.15 Use of Electronic Mail (E-mail)
PS-06.20 Security of Data
PS-10 Internal and External Communications/Advertisements
PS-30 Privacy Rights of Students (Buckley Amendment)
PS-40 Employee Records Confidentiality PS-
51 Confidentiality in Sponsored Projects PS-
74 Records and Archives
PS-101 Appropriate Use of University Equipment and Property
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
S.B. 205 (signed into law July 12, 2005; effective January 1, 2006, Act 499)