POLICY STATEMENT 107
COMPUTER USERS' RESPONSIBILITIES

POLICY DIGEST

Monitoring Unit:
Initially Issued: January 2, 2003
Last Revised: April 1, 2016

I. PURPOSE

This Policy Statement applies to all *users* of *computing resources* at, for, or through Louisiana State University regardless of *user's* affiliation or relation with the University, and irrespective of where the resources are located, utilized, or accessed. Specifically, this policy statement establishes important guidelines and restrictions regarding any and all use of *computing resources* 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 *computing resources* provided at, for, by and/or through the University, as well as those *computing resources* existing throughout the world to which the University provides and/or enables access. The University provides *computing resources* and access to *computing resources* for authorized *users* to support the academic, educational, public service, and research initiatives of the institution. No use of the *computing resources* shall conflict with the academic, educational, public service, and research initiatives of the University or with applicable laws and regulations. As a condition of use and access to *computing resources*, each *user* shall comply with this Policy Statement.

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:

A. the LSU network peripherals, and related equipment and software

B. *data* communications infrastructure, peripherals, and related equipment and software;

C. voice communications infrastructure, peripherals, and related equipment and software;

D. 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 and data that is used by or belongs to the University or that is processed, stored, maintained, transmitted, copied on, or copied from University *computing resources*.

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

IP spoofing: shall be defined as a technique used to gain unauthorized access to computers, whereby an intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

ITS: shall refer to Louisiana State University Information Technology Services.

Packet capturing: shall be defined as any unauthorized monitoring of *data* traveling over the network.

Port scanning: shall be defined as scanning a computer's ports (place where information goes into and out of a computer) to identify open doors to a computer. *Port scanning* has legitimate uses in managing networks, but unauthorized *port scanning* is strictly prohibited.

Security breach: shall be defined as any known or suspected compromise of the security, confidentiality, or integrity of *data* or *computing resources* that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and/or access to *data*. Good faith access or acquisition of *data* by an individual or *functional unit* is not a *breach* of the security of the system, provided that the information is not improperly used, or subject to subsequent unauthorized access, use, or disclosure.

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

III. GENERAL POLICY

Use of the University's *computing resources* and network capacity is a privilege, not a right. LSU may limit access to and/or review and monitor its *computing resources* and the use of *computing resources*, without notice to or authorization from *user(s)*, for any reason including *user(s)* failure to comply with applicable laws and/or University policies and directives. LSU may disclose information pertaining to use of its *computing resources* to University administration, law enforcement, investigating authorities, and others as LSU deems appropriate.

By law, the University must preserve the confidentiality of certain *data* and information it maintains about individuals attending or working at the University. However, *users* should not have an expectation of absolute privacy regarding their use of *computing resources* or information or *data* stored on the University's *computing resources as outlined in PS 114,* and the University specifically reserves the right, in the course of technical, civil, or criminal investigations to review and copy any *data* or other information stored on any *computing resources*, without notice to or consent from any *user,* by use of forensic techniques or otherwise.

To facilitate the security of *data* and *computing resources* and compliance with this Policy Statement, the University may monitor all usage of the Internet on or through *computing resources* and all other use of the University's *computing resources*, including, without limitation, reviewing a list of any and all Internet sites accessed by any *user* and all e-mails transmitted and/or received on any *computing resources*. University students, employees, contractors, and vendors are subject to legal and/or disciplinary action as a result of any use of *computing resources* that is illegal, unauthorized, or in violation of this or any other University policy or directive up to, and including, termination or expulsion.

A. Appropriate Use

Each *user* is responsible for adhering to the highest standards of ethical, responsible, and considerate use of *computing resources*, and for avoiding those uses prohibited by law or by policies or directives of the University. Under no circumstances can University *computing resources* be used for illegal or unauthorized purposes.

Specifically, each *user* of *computing resources* shall:

1. Use *computing resources* only for authorized purposes in accordance with LSU's policies and procedures, with federal, state, and local laws, and with regulations by authorities governing the use of *data*, *computing resources*, software, e-mail and/or similar technology.

2. Secure and maintain computer accounts, passwords, and other types of authorization in confidence, and inform *ITS* immediately if a known or suspected *security breach* occurs.

3. Maintain confidential and other protected or proprietary *data* and information, particularly which prescribed by law and University policy, in accordance with appropriate security measures.

4. Be considerate in the use of shared *computing resources* and network capacity, coordinating with *ITS* for "heavy use" operations that may slow operations for other *users*.

5. Accept full responsibility for any publication resulting from the use of *computing resources* and/or publishing Webpages and similar resources, and ensure that all copyrights and trademarks have been authorized for use.

B. Misuse or Abuse

Appropriate University administrative offices may establish and maintain procedures necessary to investigate, receive, and resolve allegations of apparent abuse or misuse of University *computing resources*. These offices include but are not limited to the Office of the Dean of Students, Human Resource Management, Information Technology Services, University Registrar, Internal Audit, and LSU Police.

Specifically, each *user* of *computing resources* shall NOT:

1. Obtain or use another's log on ID or password, or otherwise access *data* or *computing resources* to which authorization has not been expressly and validly given. *Users* shall not use another's log on identification or password to hide their identity or attribute their use of *data* or *computing resources* to another.

2. Copy, install, or use any software, *data*, files, or other technology that violates a copyright or license agreement. In particular, each *user* should not distribute or download copies of copyrighted material for entertainment or personal use without explicit permission from the copyright owner.

NOTE: *Copyright law applies to materials such as games, movies, music, or software in both analog and digital format.* ***User(s) shall not download an illegally distributed file to a computing resource.*** *Copyright holders regularly notify Louisiana State University of infringing activity using the procedures outlined in the Digital Millennium Copyright Act of 1998 (DMCA) and other legal procedures. As a service provider, Louisiana State University must investigate complaints and take action to remove unlawful material. The law provides means for a copyright owner to obtain the identity of a subscriber****. If you illegally possess or share copyrighted materials, you may be denied access to Louisiana State University's computing resources, be subject to disciplinary actions via the Office of the Dean of Students and/or Human Resource Management, and possibly face civil and/or criminal legal proceedings and sanctions. Please see http://www.copyright.gov/legislation/dmca.pdf for more information.***

3. Utilize *computing resources* to create, transmit, or otherwise participate in any pranks, chain letters, false or deceptive information, misguided warnings, pyramid schemes, or any fraudulent or unlawful purposes.

4. Utilize *computing resources*, including the Internet and/or e-mail, to access, create, transmit, print, or download material that is defamatory, obscene, fraudulent, harassing (including uninvited amorous or sexual messages), threatening, incites violence, or contains slurs, epithets, or anything that may be reasonably construed as harassment or disparagement based on race, color, national origin, sex, sexual orientation, age, disability, or religion or to access, send, receive, or solicit sexually oriented messages or images or any other communication prohibited by law or other University directive.

5. Intentionally or knowingly copy, download, install, or distribute a computer virus, worm, "Trojan Horse" program, or other destructive programs, or otherwise harm systems or engage in any activity that could reasonably and foreseeably disrupt services, damage files, cause loss of *data*, or make unauthorized modifications.

6. Monopolize or disproportionately use shared *computing resources*, overload systems or networks with endless loops, interfere with others' authorized use, degrade services, or otherwise waste computer time, connection time, disk space, or similar resources.

7. Add, modify, reconfigure, or extend any component of the University network (e.g. hubs, routers, switches, wireless access points, firewalls, etc.) without express, written authorization from *ITS*.

8. Accept payments, discounts, free merchandise, or services in exchange for any services provided through use of the *computing resources*, unless expressly authorized in writing by the Vice President of Finance & Administration and CFO.

9. Endanger the security of any *data* or *computing resources* or attempt to circumvent any established security measures, for any reason, such as using a computer program to attempt password decoding. *Users* must not acquire, store, or transmit any hardware or software tools that are designed to compromise the security of *computing resources* without the express written authorization of *ITS*.

10. Send unsolicited mass mailings or "spamming." Mass mailings should only be sent to clearly identified groups for official purposes, and may not be sent without proper authorization and coordination (for example, disseminating administrative announcements, notifying students of educational opportunities, or LSU organizations sending announcements to their members).

11. Utilize *computing resources* to develop, perform, and/or perpetuate any unlawful act or to improperly disclose confidential information including, but not limited to, *IP spoofing*, *packet capturing* and *port scanning*.

12. Install, store, or download software from the Internet or e-mail to University *computing resources* unless such conduct is consistent with the University's educational and academic policies or otherwise approved by *ITS*, in writing.

13. Copy, impair, or remove any software located on any *computing resources* or install any software on any *computing resources* that impairs the function, operation, and/or efficiency of any *computing resources*.

14. Utilize or access *computing resources* or *data* anonymously or withshared *user* identifications.

15. Engage in any acts or omissions to intentionally or unreasonably endanger or damage any *data* or the security or integrity of any *data* or *computing resources*.

16. Allow or assist others to utilize *computing resources* in a manner that is in violation of this Policy Statement.

17. Access, add, or modify any *data* without proper authorization.

18. Utilize *computing resources* or *data* in furtherance of, or in association with, any crime or violation of the Code of Student Conduct or other University policy or directive.

19. Utilize University *computing resources* to promote, solicit, support or engage in any commercial activities on behalf of or for the benefit of any person or entity other than the University

IV. ELIGIBILITY

In general, access to *computing resources* is provided to the following groups:

A. Active faculty, staff, and students in support of University operations and initiatives. The eligibility of these individuals to access *computing resources* may be tested automatically and periodically against University records. Other sources may be used where these databases do not accurately reflect an ongoing affiliation.

B. Persons not affiliated with LSU engaged in research or support of University operations or University supported initiatives. The eligibility of these individuals to access *computing resources* and/or *data* requires initial and periodic verification of need by a Dean, Department Head, or Director. Requests must be accompanied by the reason for the access, the name and contact information of the sponsoring Dean, Department Head, or Director, and the length of time for

which the access will be required.

C. Access to *computing resources* by retired faculty and staff is a recognized benefit to the University community as long as providing these resources is economical and does not adversely affect the operations of the University. This statement applies primarily to electronic mail and general purpose academic or research systems. In the event that resources become constrained, this practice may be eliminated or restricted. However, the University, in its sole discretion, at any time may limit, withdraw, or deny access to retired faculty and staff.

NOTE: *Colleges, departments, and other administrative units may issue local technology policies and procedures that support their organizational missions and requirements. Such policies may be more restrictive than University policy, but CAN NOT be more permissive. All local technology policies and procedures should be sent to the IT Security & Policy Officer in the Office of the Associate Vice President for Information Technology for review.*

V. PROCEDURES

A. Appropriate Use

Consultation: The IT Security & Policy Officer in the Office of the Associate Vice President for Information Technology at Louisiana State University is available to provide advice and consultation related to technology use, including the use of *computing resources*.

B. Misuse or Abuse

Reporting: *Security breaches* and apparent or suspected misuse or abuse of LSU *computing resources* should be immediately reported to the Office of the Associate Vice President for Information Technology. The IT Security & Policy Officer represents the Associate Vice President for Information Technology with respect to these issues. Where violations of the policies and procedures governing *computing resources* and/or of law are alleged, appropriate law enforcement and/or University administrative offices may be contacted.

Technical Investigation: When technical investigation or computer forensics is required, the IT Security & Policy Officer will coordinate the gathering and interpretation of relevant information. All investigations will proceed in accordance with applicable University practices, policies, procedures, and in compliance with applicable laws protecting the privacy of any education or other personally-identifiable records or *data* involved in the incident.

Sanctions: Violations may result in sanctions, such as terminating access to *computing resources*, disciplinary action, civil liability, and/or criminal sanctions. All *users* are specifically prohibited from taking any steps that block the University's access to files and *data*, other than the use of University passwords or approved encryption programs, unless such conduct is consistent with the University's educational and academic policies or otherwise properly approved by the University. The University may temporarily suspend or block access to any account, *data,* or *computing resources* prior to the initiation or completion of such procedures when it is reasonable to do so in order to protect *data* or the integrity, security, and functionality of *computing resources*, or to otherwise protect the University or its students and employees.

C. Eligibility

Requests for access to *ITS* managed *computing and networking resources* should be directed to the

ITS HelpDesk. The IT Security & Policy Officer in the Office of the Vice Chancellor for Information Technology at Louisiana State University is also available to provide advice and policy interpretation to any member of the LSU community in these situations.

Requests for access to *computing resources* not managed by *ITS* should be directed to the administration office where the service is located. Additionally, requests for use of other technology services (i.e., computers and copy machines) within a specific departmental area should be directed to the Dean, Department Head, or Director of the department in which the service is located.

1. Faculty and staff may access and use LSU *computing resources* until the termination of their affiliation with LSU. Renewal is automatic and is based on University records. *User(s)* whose status as a student or employee has been terminated by the University are no longer authorized to utilize *computing resources*, even if their access has not been blocked by technology services.

2. Retired faculty and staff may be provided access and use LSU *computing resources,* in the sole discretion of the University, as long as there are resources available to support their continued use. However, the University may limit, withdraw, or deny access to retired members of its faculty and staff in its sole discretion. Renewal is automatic and is based on continued active account use and University records. If a resource supporting "active" *users* becomes constrained and the number of accounts belonging to retired members must be reduced, account use and longevity will be used as the criteria for removing accounts as necessary to recover appropriate resources.

3. Students may access and use LSU *computing resources* until they graduate or are not enrolled for two consecutive semesters (not including Summer). A student's account will be disabled after one inactive semester, and purged after the last enrollment period of the second semester for which the student is not enrolled. Enrollment is determined using University records.

4. The University, in its sole discretion, may provide limited access to *computing resources* for specialized purposes, such as conference attendees, external entities under contract to Louisiana State University, or visitors. A sponsor must be identified on any computer account provided for this purpose, and the sponsor must be a Dean, Department Head, or Director.

5. Alumni of Louisiana State University are NOT eligible to use *computing resources* unless eligible under another category.

6. Usernames MAY BE RE-USED after the accounts remain inactive for two years. *User(s)* have no expectation of privacy or property right or interest in any *username* assigned or approved by the University or in their continued use of or access to *computing resources*.

Questions or comments regarding this policy statement should be submitted, in writing, to the Office of the Associate Vice President for Information Technology.

VI. SOURCE

The Louisiana Database Security Breach Notification Law (Act 499)