POLICY STATEMENT 114
SECURITY OF COMPUTING RESOURCES

POLICY DIGEST

Monitoring Unit: Information Technology Services
Initially Issued: October 3, 2006
Last Revised: April 1, 2016

I. PURPOSE

This Policy Statement outlines the role and authority of Information Technology Services (ITS) in supporting and upholding the security and integrity of the Louisiana State University information technology (IT) environment.

IT has become critical in support of most if not all of LSU operations, which has resulted in a very complex, distributed, and diverse technology environment. *Data* is continuously being stored, accessed, and manipulated electronically, which increases the risk of unauthorized access, disclosure, or modification of *data*.

Institutions of higher education are subject to various regulatory requirements designed to protect the privacy of education records, financial information, medical records, and other personal information maintained by the University relative to its students and employees. Further, the University seeks to maintain as confidential certain research *data*, intellectual property, and other proprietary information owned, licensed, or otherwise maintained or used by the University. Systems that are not properly secured are subject to misuse and/or unauthorized access. Everyone associated with providing and using information technology services should be diligent in their protection of *data*, use of *computing resources*, administration and maintenance of systems, response to security threats, and compliance with PS-107 and other policies and directives. Information related to intrusions, attempted intrusions, unauthorized access, misuse, or other abnormal or questionable incidents should be quickly reported to Information Technology Services, so the event can be recognized, mitigated, and hopefully avoided elsewhere.

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; 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 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*.

Protected information*:* shall be defined as *data* or information that has been designated as private, protected, 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 individually 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.

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

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*. This requirement is especially important for those *computing resources* that support or host critical business functions or *protected information*.

The IT Security & Policy Officer in Information Technology Services has the authority: (i) to develop and implement policies necessary to minimize the possibility of unauthorized access to *protected information* and the LSU's information technology infrastructure; (ii) to consult and educate *user(s)* and *functional unit(s)* relative to their individual and collective responsibilities to protect *data* and secure *computing resources*; and (iii) to take reasonable actions to mitigate incidents or concerns relating to security of *data* or *computing resources*. This includes establishing guidelines, procedures, standards, and security resources, conducting security audits, and providing consulting services to *functional unit(s)* for all LSU computer systems or other *computing resources*.

User(s) within *functional unit(s)* are required to report any *suspected or known security breaches* or flaws relating to the security of University *computing resources* to the *IT Security & Policy Officer*. The IT Security & Policy Officer will assess reported breaches and flaws and provide advice as to an appropriate response. A failure to report suspected or known *security breaches* or flaws is cause for disciplinary action, including termination of employment. *Users* should immediately discontinue any use of *computing resources* or practice that could reasonably lead to a *security breach*.

The *IT Security & Policy Officer* has the authority to assume control over the response to any suspected

or known *security breach* or flaw involving LSU's information technology infrastructure, *data*, and *computing resources* regardless of the *functional unit* involved. Appropriate remedies may be taken to secure the *computing resources* and mitigate any unauthorized use, disclosure, or access to *data*, including the removal of devices to more secure facilities and denying access to *computing resources* and/or *data*. This authority will be exercised if the IT Security & Policy Officer determines that the *functional unit* does not have the means and/or ability to access and/or react appropriately in a timely manner to a specific security incident. The IT Security & Policy Officer may draw upon the experience, expertise, and resources of other University *functional units* when necessary and as appropriate.

IV. PROCEDURES

Intrusion attempts, *security breaches*, and other security related incidents or flaws perpetrated against or involving *computing resources* either attached to a LSU operated network or in a *functional unit* shall be reported IMMEDIATELY to the *Network Operations Center (NOC).* This is CRITICAL for systems supporting vital functions and/or hosting institutional or *protected information*. *User(s)* within *functional unit(s)* must:

A. Report any *security breaches* in order to obtain advice and assistance,
B. Report any systematic unsuccessful attempts (i.e. log in attempts, probes, or scans), and
C. When feasible, send detailed reports as soon as the situation is detected.

Upon receiving a report, the Network Operations Center and IT Security & Policy Officer will respond according to ITS standard operating procedures.

In order to protect University *data* and systems, as well as to protect threatened systems external to the University, the IT Security & Policy Officer may place limits or restrictions on technology services provided on or from any *computing resources*.

A. Limitations may be implemented through the use of policies, standards, and/or technical methods, and could include (but may not be limited to) usage eligibility rules, password requirements, or restricting or blocking certain protocols or use of certain applications known to cause security problems.

B. Restrictions may be deployed permanently based on continuing threat or risk after appropriate consultation with affected constituents, or they may be deployed temporarily, without prior coordination, in response to an immediate and serious threat.

C. Restrictions deployed temporarily will be removed when the risk is mitigated to an acceptable level, or where the effect on LSU functions caused by the restriction approaches or exceeds risk associated with the threat.

In order to protect LSU *data* and systems, as well as to protect threatened systems external to the LSU, the IT Security & Policy Officer may unilaterally direct that a specific *computing resource* be isolated from LSU, campus, or external networks, given:

A. Information reasonably points to the system as having been compromised.

B. There is ongoing activity associated with the system that is causing or will cause damage to other University *computing resources* or *data*, or to systems of other internal or external *users*, or where there is significant risk of such damage occurring.

C. All reasonable attempts have been made to contact the responsible technicians or *functional unit* management, or contact has been made, but the technician or *functional unit* managers are unable to or choose not to resolve the problem in a reasonable time.

Isolation is removed when the risk is mitigated to an acceptable level, or where loss of access or function caused by the isolation approaches or exceeds risk associated with the threat, as determined between the responsible *functional unit* and the IT Security & Policy Officer.

All *security breaches*, incidents, or concerns should be reported immediately to security@lsu.edu and to the Network Operations Center at 225-578-6621.

V. SOURCES

PM-36 Louisiana State University System Information Security Plan
The Louisiana Database Security Breach Notification Law (Act 499)