**Policy: Computer Use Rules**

**Purpose**

This Policy applies to all *users* of *computing resources* at, for, or through \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [School Name] regardless of the *user’s* affiliation or relation with the School, and irrespective of where the resources are located, used, or accessed.

This policy outlines specific responsibilities that each *authorized* *user* acknowledges, accepts, and agrees to follow when using *computing resources* provided at, for, by or through the School, as well as those *computing resources* existing throughout the world to which the School provides or enables access.

No use of the *computing resources* shall conflict with the academic, educational, public service, and research initiatives of the School or with applicable laws and regulations. As a condition of use and access to *computing resources*, each *user* shall comply with this Policy.

**Definitions**

For the purposes of this Policy, the following definitions shall apply: **“*Computing resources*”** shall be defined as all devices (including, but not limited to, personal computers, laptops, tablets, PDAs, and smart phones) owned by the School, the *user* or otherwise, which are part of or are used to access (1) the School’s 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 School. *Computing resources* or components thereof may be individually assigned or shared, single-user or multiuser, stand-alone or networked, or mobile or stationary.

***“Data”*** shall include all information and *data* that is used by or belongs to the School or that is processed, stored, maintained, transmitted, copied on, or copied from School *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 the School 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 the School’s Information Technology (Computer) 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 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 uses *computing resources, including, but not limited to, employees, faculty, staff, agents, vendors, consultants, contractors, or subcontractors of the School.*

**General Policy**

Use of the School’s *computing resources* and network capacity is a privilege, not a right. The School may limit access to 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 or School policies and directives. The School may disclose information pertaining to use of its *computing resources* to School administration, law enforcement, investigating authorities, and others as the School deems appropriate.

U*sers* should not have an expectation of absolute privacy regarding their use of *computing resources* or information or *data* stored on the School’s *computing resources,* and the School 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, the School may monitor all usage of the Internet on or through *computing resources* and all other use of the School’s *computing resources*, including, without limitation, reviewing a list of any and all Internet sites accessed by any *user* and all e-mails transmitted or received on any *computing resources*. School students, employees, contractors, and vendors are subject to legal or disciplinary action as a result of any use of *computing resources* that is illegal, unauthorized, or in violation of this or any other School policy or directive up to, and including, termination or expulsion.

1. **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 School. Under no circumstances can School *computing resources* be used for illegal or unauthorized purposes. Specifically, each *user* of *computing resources* shall:

* Use *computing resources* only for authorized purposes in accordance with the School’s policies and procedures, and with all laws and regulations governing the use of *data*, *computing resources*, software, e-mail or similar technology.
* 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.
* Maintain confidential and other protected or proprietary *data* and information.
* 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*.
* Accept full responsibility for any publication resulting from the use of *computing resources* or publishing Web pages and similar resources, and ensure that all copyrights and trademarks have been authorized for use.
1. **Misuse or Abuse**

Appropriate School administrative offices may investigate, receive, and resolve allegations of apparent abuse or misuse of School *computing resources*.

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

* 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.
* 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.
* Use *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.
* Use *computing resources*, including the Internet 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 School directive.
* 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.
* 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.
* Add, modify, reconfigure, or extend any component of the School network (e.g. hubs, routers, switches, wireless access points, firewalls, etc.) without express, written authorization from *ITS*.
* 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*.
* 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 School organizations sending announcements to their members).
* Use *computing resources* to develop, perform, or perpetuate any unlawful act or to improperly disclose confidential information including, but not limited to, *IP spoofing*, *packet capturing* and *port scanning*.
* Install, store, or download software from e-mail or the Internet to School *computing resources* unless such conduct is consistent with the School’s educational and academic policies or otherwise approved by *ITS*, in writing.
* Copy, impair, or remove any software located on any *computing resources* or install any software on any *computing resources* that impairs the function, operation, or efficiency of any *computing resources*.
* Use or access *computing resources* or *data* anonymously or with shared *user* identifications.
* Intentionally or unreasonably endanger or damage any *data* or the security or integrity of any *data* or *computing resources*.
* Allow or assist others to use *computing resources* in a manner that is in violation of this Policy.
* Access, add, or modify any *data* without proper authorization.
* Use *computing resources* or *data* in furtherance of, or in association with, any crime or violation of any School policy or directive.
* Use School *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 School
1. **Eligibility**

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

* Active faculty, staff, and students in support of School operations and initiatives.
* Persons not affiliated with the School, engaged in research or support of School operations or School supported initiatives. Requests to *ITS* for the access must be accompanied by the reason, 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.
* Access to *computing resources* by retired faculty and staff is a recognized benefit to the School community as long as providing these resources is economical and does not adversely affect the operations of the School.

***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 School policy, but* cannot be more permissive*. All local technology policies and procedures should be sent to the ITS for review.*

**Procedures**

1. **Appropriate Use**

**Consultation:** The School’s ITS is available to provide advice and consultation related to technology use, including the use of *computing resources*.

1. **Misuse or Abuse**

**Reporting:** *Security breaches* and apparent or suspected misuse or abuse of School *computing resources* should be immediately reported to ITS. Where violations of the policies and procedures governing *computing resources* or of law are alleged, appropriate law enforcement or School administrative offices may be contacted.

**Sanctions:** Violations may result in sanctions, such as terminating access to *computing resources*, disciplinary action, civil liability, or criminal sanctions. The School 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 School or its students and employees.

1. **Eligibility**

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

* Faculty and staff may access and use School *computing resources* until the termination of their affiliation with the School. Renewal is automatic and is based on School records. *User(s)* whose status as a student or employee has been terminated by the School are no longer authorized to use *computing resources*, even if their access has not been blocked by technology services.
* Retired faculty and staff may be provided access and use School *computing resources,* in the sole discretion of the School, as long as there are resources available to support their continued use. Renewal is automatic and is based on continued active account use and School records.
* Students may access and use School *computing resources* until they graduate or are no longer enrolled.
* The School, 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 School, 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.