TULANE UNIVERSITY SCHOOL OF LAW
POLICY ON THE USE OF COMPUTERS AND NETWORKS

Tulane University School of Law maintains its computer system and network connectivity for faculty, students, and staff in pursuit of the academic missions of the law school, and for staff to work to support these endeavors. In addition to the following policies and standards, the Tulane University Computing Information & Dissemination Acceptable Use Policy (Appendix 1) applies to members of the law school community.

Part I

A. Introduction

This acceptable-use policy governs the use of computers and networks on the Tulane School of Law campus. As a user of these resources, faculty, staff, and students are responsible for reading and understanding this document. This document protects the consumers of computing resources, computing hardware and networks, and the system administrator.

Computer facilities and infrastructure are provided for meeting academic goals and to provide access to local, national, and international facilities to aid in the achieving of these goals. Those using the facilities and services must respect the intellectual and access rights of others locally, nationally, and internationally. Students should be aware that any use of the facilities or infrastructure that is in violation of the guidelines listed below may be considered an Honor Code violation.

The School of Law is committed to intellectual and academic freedom and to the application of those freedoms to computer media. The School of Law is also committed to protecting the privacy and integrity of computer data and records belonging to the School of Law and to individual users.

For purposes of this Policy, the term "component of the School of Law network" shall include workstations (including library research workstations, Lexis and Westlaw terminals), and all peripheral devices (including printers, mice, modems, speakers, keyboards, monitors, network outlets, cabling, etc.).

B. Rights and Responsibilities

Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Because electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements and copyright laws.

C. Existing Legal Context

All existing laws (federal and state) and Tulane University regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct. See, for example, Law School Library Information Guide ("Library Rules and Policies") and Tulane Law School Student Handbook. Users do not own accounts on Tulane University computers, but are granted the privilege of exclusive use. Under the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2520 et seq.), users are entitled to privacy regarding information contained on these accounts. This act, however, allows the system administrator or other University employees to access user files in the normal course of their employment when necessary to protect the integrity of computer systems or the rights or property of the University. For example, the system administrator may examine or make copies of files that are suspected of misuse or

that have been corrupted or damaged. User files may be subject to search by law enforcement agencies under court order if such files contain information which may be used as evidence in a court of law. In addition, student files on University computer facilities are considered "educational records" under the Family Educational Rights and Privacy Act of 1974 (20 U.S.C. § 1232[g]).

Misuse of computing, networking, or information resources may result in the loss of computing and/or network access. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable University policies, procedures, or collective bargaining agreements. Illegal reproduction of software and other intellectual property protected by U.S. copyright law is subject to civil damages and criminal punishment, including fines and imprisonment. The School of Law supports the policy of EDUCOM on "Software and Intellectual Rights" (Appendix 2).

Other organizations operating computing and network facilities that are accessible via the School of Law network may have their own policies governing the use of those resources. When accessing remote resources from school facilities, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations.

D. Enforcement

The system administrator is initially responsible for protecting the system and users from abuses of this policy. Pursuant to this duty, the system administrator may informally or formally communicate with offending parties. In more extreme cases, the system administrator may temporarily revoke or modify use privileges. Suspension decisions will be reviewed by the Dean or the Dean's designee.

Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the system administrator. This may be done through electronic mail or in-person discussion and education.

Repeated minor infractions, or misconduct which is more serious, may result in the temporary or permanent loss of computer-access privileges or the modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computer resources, vandalization of equipment or software, attempts to steal passwords or data, unauthorized use or copying of licensed software, unauthorized installation of software onto the system or individual units (e.g., games, screen savers), repeated harassment, or threatening behavior.

In addition, offenders may be referred to their supervisor or department head, Dean, employer, or other appropriate University officer for further action. If the individual is a student, the matter may be referred to the Honor Board for disciplinary action.

Any offense which violates local, state, or federal laws may result in the immediate loss of all School of Law computing privileges and will be referred to appropriate School of Law offices and/or law enforcement authorities.

Part II

A. Conduct Which Violates this Policy

Conduct which violates this policy includes, but is not limited to, the activities in the following list.

1. Unauthorized use of a computer system or resources.
2. Destruction of any component of the School of Law network.
3. Using the School of Law network to gain unauthorized access to any computer systems.

4. Connecting any equipment, or installing any software, program, or code, to the School of Law network without the express prior authorization of the system administrator.

5. With respect to any workstation located in the School of Law computer lab (including library reference workstations, and Lexis and Westlaw terminals), any attempt to connect any equipment or to install or store any software, program, data or code. "Data" includes documents, spreadsheets, graphics, and archived files.

6. Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.

7. Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks. This includes, but is not limited to, physical tampering with or destruction of any component of the School of Law network.

8. Knowingly or carelessly running or installing on any computer or network, or giving to another user, a program intended to damage or to place excessive load on a computer or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms.

9. Deliberately wasting or overloading computing resources, such as printing too many copies of a document.

10. Violating terms of applicable software licensing agreements or copyright laws. The latter includes the violation of copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc.

11. Using School of Law computing resources for commercial activity, such as creating or advertising products or services for sale in any area not designated by the system administrator for such activity.

12. Using electronic mail to harass, threaten, defraud, or otherwise harm another. This includes sending repeated, unwanted electronic mail to another user.

13. Initiating, republishing or propagating electronic chain letters, of whatever content or message.

14. Except in any area such as an electronic bulletin board designated by the system administrator for such activity, mass mailings are prohibited. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g., "spamming," "flooding," or "bombing."

15. Forging, or attempting to forge, the identity of a user or machine in an electronic communication.

16. Transmitting or reproducing materials that are slanderous or defamatory in nature, or that otherwise violate existing laws or university regulations.

17. Displaying obscene, lewd, or sexually harassing images or text in a public computer facility or location that is in view of others.

18. Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

19. Allowing any other individual to use one's law school user identification and/or password.

B. Review and Further Publication

It is the intention of the faculty of the School of Law, in adopting this policy, that it should be reviewed annually.

Part III

A. Publishing Guidelines for the World Wide Web

1. Policy Statement

The School of Law recognizes the value and potential of publishing on the Internet, and so allows and encourages student organizations, staff, and faculty to publish appropriate electronic information. Recognized student organizations may create electronic home pages or other pages that support the School of Law's mission. All electronic pages must be approved by the system administrator, with any controversial page being reviewed by the designated subcommittee of the Committee on Computers and Technology. Contents of all electronic pages must be consistent with Tulane University and School of Law policies, as well as local, state, and federal laws.

Such "contents" include links to other pages or computers. In other words, a page may be considered in violation if it contains links to a page that violates the policy.

All home pages and pages that are the electronic equivalent of a publication must begin with the title "Tulane University School of Law." These pages must also contain the date of the last revisions and will clearly communicate the name of the entity publishing the page. Further, the following statement must appear on all home pages: "The views and opinions expressed in this page are those of the page author. The contents of this page have not been reviewed by Tulane University School of Law."

Copyright laws apply to electronic publishing as well as to print publishing. Publishers must have permission to publish the information, graphics, or photographs on their pages if the publisher is not the author or creator. Electronic publications are subject to the same Tulane University policies and standards as are print publications. See also Appendix 3.

School of Law resources may not be used to create web pages for personal business or personal gain, except as may be permitted by other University policies.

The official Tulane University School of Law home page will not link directly to personal pages. When requested, users must deactivate links to material that violates this policy. The authors of personal pages must follow the guidelines in this policy.

2. Reason for Policy

The quality of information published by the School of Law plays an important role in maintaining its reputation and image. This policy sets minimal standards that are meant to ensure that information published electronically follows the same high standards as do other forms of published school information (print, audiovisual, etc.).

The School of Law complies with applicable local, state, and federal laws.

B. Independent Domain Name

Any Tulane Law School student organization that wishes to purchase an independent domain name to provide direct access to that organization's web pages contained on the Tulane Law School web site and stored on the Tulane Law School web server is permitted to do so under the following requirements. First, only domain names with the ".org" or ".edu" extension will be permitted. Domain names with the ".com" are strictly forbidden. Second, both the student organization's faculty advisor(s) and the Law School Director of Technology must approve the specific title of the domain name before it can be purchased. Third, it is the specific responsibility of the sponsoring student organization to obtain, purchase, renew and

otherwise update the domain name. Finally, the domain name can only be used to link directly to the sponsoring student organization's web pages that are contained within the Tulane Law School web site and are stored on the Tulane Law School web server.

APPENDIX 1

Tulane University

Fall 2016

Computing Information & Dissemination
Tulane University Acceptable Use Policy

The most up to date version of this policy can always be found at:
http://isowiki.tulane.edu/Tulane_Information_Security_Policies/Tulane_University_Acceptable_Use_Policy

1. PURPOSE

Tulane University provides computing resources to faculty, staff, students and affiliates for academic and administrative use in support of the mission of the University to create, communicate and conserve knowledge. The University strives to provide a robust, resilient and reliable information technology infrastructure to enable excellence in scholarship and education through the effective and innovative use of computers and information technology. Because computing and network resources are shared and limited, individuals should use the systems responsibly in pursuit of academic and administrative functions, and in doing so, are not to infringe on the rights, integrity or privacy of others or their data. In using the computing systems and network, individuals and groups must abide by standards of lawful and ethical behavior.

2. AGREEMENT

By using Tulane's computing systems and network, each person agrees that information they post on or distribute through the systems or network contains: no obscene or indecent material; no advertising material or promotional material for products or services; no material which constitutes libel, slander or invasion of privacy or publicity rights; no violation of copyrights or trademarks; no incitement to riot or violence; no violation of University policies and regulations; and no violation of federal, state or local law. Each person also consents to the following:

• *Respect for system security*. It is your responsibility to protect the integrity and security of the data in your account and observe all network security practices as required by the University.

You, and you alone, accept responsibility for all matters pertaining to the proper use of your account; this includes choosing safe passwords and ensuring that file protections are set correctly. You agree not to give away your user id and password, for any reason, or under any circumstance. You agree not to use someone else's account, either with or without permission.

• *Responsible use of computing and networking*. You agree not to obstruct any others' work by using unnecessarily large amounts of network resources (such as bandwidth and storage space) or deliberately act in a manner that will cause harm to the network. You agree not to send spam, chain letters, or other mass unsolicited mailings. You agree not to advertise or conduct non-University business using university resources unless approved by an authorized University official.

• *Respect for copyright*. Unauthorized distribution of copyrighted material is a violation of federal law. In accordance with the Digital Millennium Copyright Act, the University, once notified of alleged copyright violations, will disconnect from the network the server or computer of the individual(s) involved. The individual who is distributing the copyrighted materials is responsible for any copyright infringement.

• *Respectful Communication*. You agree to communicate only in ways that are kind and respectful. You agree to not intentionally access, transmit, copy, or create material that violates applicable laws or the University's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass).

• *Respect for Tulane's computing systems and network administration.* You agree to use the systems and network in a way which promotes Tulane's academic mission. Accordingly, you acknowledge and consent that, when it is necessary to perform systems administration, or, in order to protect Tulane's legal interests, network administrators may access your files and data on the Tulane computing systems and network. In addition, you consent to monitoring and review of your user id, user activity, files and data on the Tulane systems and network, as well as Tulane's right to "freeze" or remove access to any files or data which Tulane reasonably believes violates User Obligations.

3. SPECIFIC PROHIBITED ACTIONS

You are given access to Tulane University's computing systems and network because they are tools to help you meet your academic and administrative goals. This access, however, is a privilege, not a right. The University reserves the right to withdraw any and all privileges in the event of a violation of this policy. Specific prohibited activities and behaviors are defined in but are not limited to the Guidelines for Acceptable Use document.

4. PENALTY FOR VIOLATION

Violations of this policy by students shall be treated as violations of the Code of Student Conduct and will be referred to the Office of the Vice President for Student Affairs for handling. Faculty and staff members who violate this policy will be subject to University disciplinary action. Tulane reserves the right to withhold computing privileges from those who do not abide by the letter or intent of this policy document. In addition, any person who violates this policy or the guidelines for interpreting this policy may also be subject to sanctions up to and including expulsion or termination.

5. APPROVAL FOR EXCEPTIONS

In the very rare instances where this policy interferes with the fulfillment of the mission of the University, Students, Faculty or Staff may request a written waiver from the Vice President of Information Technology or designee.

6. ADDITIONAL INFORMATION

For further information about this and other information security policies and applicable computing laws and regulations please contact the Information Security Officer at (504) 988-8500, or security@tulane.edu.

APPENDIX 2

The Educom Code

Software and Intellectual Rights

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy and right to determine the form, manner, and terms of publications and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasions of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

APPENDIX 3

Copyright Permissions

Portions of the Tulane University School of Law Acceptable Use Policy (Parts I and II) were adapted, with permission, from the University of California at Davis. Portions of the WWW Publishing Guidelines (Part III) were adapted, with permission, from the University of Minnesota.