WEST VIRGINIA STATE UNIVERSITY BOARD OF GOVERNORS

West Virginia State University

BOG Policy #53

Title: Responsible Use of University Computing Resources

Section 1. General

1.1 As a part of the physical and social learning infrastructure, West Virginia State University acquires, develops, and maintains computers, computer systems, and networks. These computing resources are intended for institution-related purposes, including:

- 1.1.1 Direct and indirect support of the University's instruction, research, and service missions; of University administrative functions;
- 1.1.2 Student and campus life activities;
- 1.1.3 Free exchange of ideas among members of the University community and between the University community and the wider local, national, and world communities.

1.2 The rights of academic freedom and freedom of expression apply to the use of University computing resources.

- 1.2.1 So, too, do the responsibilities and limitations associated with those rights.

1.3 The use of University computing resources, like the use of any other University-provided resource and like any other University-related activity, is subject to the normal requirements of legal and ethical behavior within the University community.

- 1.3.1 Thus, legitimate use of a computer, computer system, or network does not extend to whatever is technically possible.

1.4 Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible.

- 1.4.1 Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

1.5 Effective date: March 29, 2005

Section 2. Applicability

2.1 These regulations apply to all users of West Virginia State networked computing resources, whether affiliated with the University or not, and to all uses of those resources, whether on campus or from remote locations.

- 2.1.1 Additional policies may apply to specific computers, computer systems, or networks provided or operated by other units of the University or to uses within specific units.

2.1.2 One should consult his/her operator or manager about the specific computer, computer system, or network in which he/she is interested, or the management of the unit for further information.

Section 3. Regulations

3.1 All users of the University computing resources must:

3.1.1 Comply with all federal, West Virginia, and other applicable law; all generally applicable University policies and rules, and all applicable contracts and licenses. (Examples of such laws, rules, policies, contracts, and licenses include the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking," and similar activities; the University's code of student conduct; the University's sexual harassment policy; and all applicable software licenses.)

3.1.1.1 Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks;

3.1.1.2 Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

3.1.2 Use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized.

3.1.2.1 Ability to access computing resources does not, by itself, imply authorization to do so;

3.1.2.2 Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding;

3.1.2.3 Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the University.

3.1.3 Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected;

3.1.3.1 Ability to access other persons' accounts does not, by itself, imply authorization to do so;

3.1.3.2 Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

3.1.4 Respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.

3.1.4.1 Although there is no set bandwidth, disk space, CPU time, or other limit applicable to *all* users of University computing resources, limits are placed on individual disk space and "bandwidth managing" is utilized to provide higher priority for computing resources critical to the University. It must be realized that the University's computing resources are finite and shared;

3.1.4.2 The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.

3.1.5 Refrain from using those resources for personal commercial purposes or for personal financial or other gain;

3.1.5.1 In the interest of making the use of IT resources a natural part of the day-to-day learning and work of all members of the University community, incidental personal use is tolerated. However, one should not use University sources of email, Internet access, and other IT services for activities of an extensive nature that are unrelated to University purposes. Excessive use of systems for recreational Internet browsing, email, or game playing is to be avoided and may subject University employees to disciplinary action;

3.1.5.2 Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

3.1.6 Refrain from stating or implying that they speak on behalf of West Virginia State University and from using WVSU trademarks and logos without authorization to do so;

3.1.6.1 Affiliation with the University does not, by itself, imply authorization to speak on behalf of the University;

3.1.6.2 Authorization to use WVSU trademarks and logos on University computing resources may be granted only by the appropriate authority. (The use of suitable disclaimers is encouraged.)

Section 4. Enforcement

4.1 Users who violate this policy may be denied access to West Virginia State computing resources and may be subject to other penalties and disciplinary action, both within and outside the University and are subject to all University policies and applicable state and federal laws (See also Section 9).

4.2 Violations will normally be handled through the institutional disciplinary procedures applicable to the relevant user.

4.2.1 The University may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University or other computing resources or to protect the University from liability;

4.2.2 The University may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Section 5. Security and Privacy

5.1 The University employs various measures to protect the security of its computing resources and of its users' accounts.

5.1.1 Users should be aware, however, that the University cannot guarantee such security;

5.1.2 Users should, therefore, engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly.

5.1.3 Users should be aware that unencrypted messages are routinely reviewed at many stages of the message transmission process both internal and external to the University.

5.2 Users should also be aware that their uses of University computing resources are not private;

5.2.1 Although the University does not routinely monitor computer and network use, the University does reserve the right to monitor computer and network use for operational needs and to ensure compliance with applicable laws and University policies. The University considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information contained on University systems or equipment that may be related to inappropriate use;

5.2.2 The University specifically monitors the activity and accounts of individual users of University computing resources, including individual login sessions and communications when:

5.2.2.1 The user has voluntarily made them accessible to the public, as by posting to the Internet via a web page or other means;

5.2.2.2 It reasonably appears necessary to do so to protect the integrity, security, or functionality of University or other computing resources or to protect the University from liability;

5.2.2.3 There is reasonable cause to believe that the user has violated or is violating this policy;

5.2.2.4 An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or

5.2.2.5 It is otherwise required or permitted by law;

5.2.2.6 Such activity is required in the normal course of network and systems operations and maintenance.

5.2.3 Any such individual monitoring other than that specified above, or required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Director of Computer Services or a University official at least at the level of Vice President.

5.3 The University may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings.

Section 6. Inappropriate Use of Computer Resources (Computer Abuse)

6.1 The following delineates activities that constitute abuse of West Virginia State (WVS) resources as established by the preceding rules regarding the use or abuse of all hardware, data, software and communications networks associated with campus computer systems:

6.1.1 Privacy - Investigating or reading another user's file is considered a violation of privacy unless in response to suspected infringement of University policy or required by a law enforcement agency or in the normal course of network and systems operations and maintenance.

6.1.1.1 Violations include but are not limited to:

- Attempting to access another user's files without permission;
- Furnishing false or misleading information or identification in order to access another user's account;
- Attempts to access WVSU computers, computer facilities, networks, systems, programs or data without authorization;
- Unauthorized manipulation of WVSU computer systems, programs or data;
- Unauthorized monitoring of network traffic, for example reading e-mail messages not addressed to the user.

6.1.2 Theft

6.1.2.1 Attempted or detected alteration of software, data or other files as well as disruption or destruction of equipment or resources is considered theft.

6.1.2.2 Violations include but are not limited to:

- Using subterfuge to avoid being charged for computer resources;
- Deliberate, unauthorized use of another users' account to avoid being billed for computer use;
- Abusing specific resources such as the Internet;
- Removing computer equipment (hardware, software, data, etc.) without authorization;
- Copying or attempting to copy data or software without authorization.

6.1.3 Vandalism. Violations include but are not limited to:

- Sending mail or a program that will replicate itself (such as a computer virus) or do damage to another user's resources;
- Sending excessive quantities of mail to a single destination or otherwise generating excessive quantities of network traffic, which have the deliberate effect of overloading a networked resource;
- Tampering with or obstructing the operation of WVSU computer systems;
- Inspecting, modifying or distributing data or software (or attempting to do so) without authorization;
- Damaging computer hardware or software.

6.1.4 Harassment. WVSU has as part of its mission, the responsibility of being a distinctive "living laboratory of human relations," attracting a racially and culturally diverse student body, faculty, and staff. The University cherishes its unique history and its reputation for safeguarding academic freedom, for being innovative in its scholastic programs, and for removing barriers to education and leadership for women, minorities, and the handicapped.

6.1.4.1 Sending or publishing in an electronic form (for example, a World Wide Web page) material that is abusive or obscene, or engaging in other forms of harassment that impedes the progress of the University’s mission and/or are detrimental to the University

community as a whole. Harassment violations include but are not limited to:

- Interfering with legitimate work of another user;
- Sending unwanted messages or files to other users after being requested not to send them;
- Sending excessive quantities of messages or files;
- Sending or publishing in an electronic form abusive or obscene messages or materials via computers;
- Using computer resources to engage in abuse of other users.

6.1.4.2 Other acts considered unethical and abusive include:

- Unauthorized and time-consuming recreational game playing;
- Using computer accounts for work not authorized for that account;
- Sending chain letters or unauthorized mass mailings;
- Using the computer for personal profit or other illegal purposes;
- Personal advertisements;
- Display of offensive material and graphics in public areas.

Section 7. Copyright and Intellectual Rights

7.1 The following reiterates West Virginia State's regulations regarding copyright and intellectual rights which apply to use of computer resources;

7.1.1 West Virginia State prohibits the copying, transmitting, or disclosing of proprietary data, software or documentation (or attempting to commit these acts) without proper authorization;

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

7.1.3 Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments.

7.1.3.1 Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret or copyright violations are grounds for sanctions against members of the academic community.

7.2 This Statement of Copyright and Intellectual Rights applies in full to the use of West Virginia State University Computer Services and its resources.

Section 8. Computer Usage Guidelines

8.1 Every user must have a valid, authorized account and may only use those computer resources for which they are specifically authorized.

8.1.1 Each user is responsible for safeguarding his/her own account;

8.1.2 A user should not allow another user to use his/her account unless authorized by the system administrator for a specific purpose;

8.1.3 A user may not change, copy, delete, read or otherwise access files or software without the permission of the owner or the system administrator.
8.1.4 A user may not bypass accounting or security mechanisms to circumvent data protection schemes.
8.1.5 A user may not attempt to modify software except when it is intended to be customized by users.
8.1.6 A user may not prevent others from accessing the system, nor unreasonably slow down the system by deliberately running wasteful jobs, playing games, or engaging in non-productive or idle computer "chatting;"

8.2 A user should assume that any software he/she did not create is copyrighted.
8.2.1 A user may neither distribute copyrighted or proprietary material without the written consent of the copyright holder, nor violate copyright or patent laws concerning computer software, documentation or other tangible assets;

8.3 A user must not use the West Virginia State University computer systems for any form of computer abuse as defined in Section 6 of this policy or to violate any rules in any appropriate West Virginia State handbooks, or to violate local, state or federal laws;

8.4 A user should promptly report misuse or abuse of computing resources or potential loopholes in computer systems security to the appropriate authorities (WVSU Computer Services Director or Computer Services personnel), and cooperate with the systems administrators in their investigation of abuse.

Section 9. Legal Ramifications

9.1 Offenders may be prosecuted under the terms described in such laws (but not limited to):
9.1.1 The Privacy Act of 1974, PL 93-579;
9.1.2 The Computer Fraud and Abuse Act of 1986, 18 USC Section 1030;
9.1.3 The Computer Virus Eradication Act of 1989, HR 5061, HR55 (amendments to 18 USC, section 1030);
9.1.4 Interstate Transportation of Stolen Property, 18 USC sections 2314 and Aiding and Abetting, 18 USC Section 2;
9.1.5 The West Virginia Computer Crimes Act.

9.2 It should be understood that this policy statement does not preclude prosecution of cases involving criminal misconduct under the laws and the regulations of Kanawha County, the State of West Virginia and the United States of America.

9.3 All violations will be reported to WVSU Public Safety Department for investigation which may result in legal and/or criminal action by state and federal authorities.