OAKLAND UNIVERSITY

ADMINISTRATIVE POLICIES AND PROCEDURES

890 - USE OF UNIVERSITY INFORMATION TECHNOLOGY RESOURCES

SUBJECT:	USE OF UNIVERSITY INFORMATION TECHNOLOGY RESOURCES
NUMBER:	890
AUTHORIZING BODY:	CHIEF OF STAFF
RESPONSIBLE OFFICE:	UNIVERSITY TECHNOLOGY SERVICES
DATE ISSUED:	JULY 2003
LAST UPDATE:	SEPTEMBER 2014

RATIONALE: This policy is intended to protect the wide array of information technology resources as defined in this Policy (Resources) provided by Oakland University (University) and to provide guidelines for the use of those Resources.

POLICY: Access to and use of Resources imposes certain responsibilities and is granted subject to University policies and procedures and federal, Michigan and all other applicable laws. Appropriate use is legal and ethical, reflects academic honesty, reflects community standards, and shows restraint in the consumption of shared resources. Appropriate use demonstrates respect for intellectual property; ownership of data; system security mechanisms; and individual rights to privacy and to freedom from intimidation, harassment, and unwarranted annoyance. Appropriate use includes instruction; independent study; research; communications; and official work of Authorized Users as defined below.

The University may, in its sole and exclusive discretion, allocate, authorize use of, and control access to Resources in differential ways in order to achieve its overall mission. This policy does not prohibit use of tools and techniques by systems administration personnel, Authorized Users, or faculty for research or instructional purposes, as long as those activities do not interfere with appropriate use by others.

SCOPE AND APPLICABILITY: This policy is intended to allow for the proper use of all Resources, effective protection of individual users, equitable access to Resources, and proper management of those Resources. It applies to all students, faculty, staff and guests using these Resources. This should be taken in the broadest possible sense.

This policy applies to University network usage even in situations where it would not apply to the computer(s) in use. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to these Resources.

Individual units at the University may add individual guidelines that supplement, but do not override or replace, this policy. In such cases, the unit should inform their users, University Technology Services (UTS) and the Office of Legal Affairs.

DEFINITIONS:

Authorized Use - Authorized Use Resources is use that the University determines, in its sole and exclusive discretion, is consistent with the education, research, and service mission of the University, consistent with effective departmental or divisional operations, and consistent with this policy.

Authorized Users - The University may control access to Resources in accordance with federal, Michigan and all other applicable laws and University policies and procedures limiting use to Authorized Users. Authorized Users may include:

(1) Current faculty, staff, and students of the University;

(2) Anyone connecting to a public information service through the use of University Resources;

(3) Others whose access furthers the mission of the University, and whose usage does not interfere with general access to Resources, as determined by the University in its sole and exclusive discretion.

Resources - Resources means the University's computing, network and information technology Resources, including without limitation all data and information in electronic format or any hardware or software that makes possible, in the broadest possible sense, the processing, transmission, storage or use of such information. As an example, included in this definition are access identity accounts and login processes; communications devices; computers; data; databases; digital images; digitized information; electronic mail; messaging; network electronics and access points; servers; software; storage devices; web sites, blogs and public information services; and workstations.

PROCEDURES:

I. INDIVIDUAL PRIVILEGES - The following individual privileges empower each of us to be productive members of the campus community. Privileges are conditioned upon acceptance of the accompanying responsibilities.

(1) Privacy - Technological methods must not be used to infringe upon privacy. However, Authorized Users must recognize that Resources are public and subject to the Freedom of Information Act, the Communications Assistance for Law enforcement Act, other federal, state and local statutes and regulations, and exceptions established by the University as permitted by law. Authorized Users utilize such Resources at their own risk.

(2) Freedom of expression - The constitutional right to freedom of speech applies to all Authorized Users of the Resources no matter the medium used.

(3) Freedom from harassment and undesired information - All constituents have the right to be free from harassment as defined in this policy by or via usage of Resources.

II. **INDIVIDUAL RESPONSIBILITIES** - Authorized Users are held accountable for their actions as a condition of continued use of Resources.

a. Demonstrating common courtesy and respect for rights of others - Authorized Users must respect and value privacy rights, behave ethically, and comply with all legal restrictions regarding the use of information that is the property of others. Compliance with all University policies regarding sexual, racial, and other forms of harassment and discrimination is required.

b. Abiding by laws, policies, contracts and licenses - Authorized Users must comply with all federal, Michigan, and other applicable laws; all generally applicable University rules and policies; and all applicable contracts and licenses. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

   Examples of such laws, rules, policies, contracts and licenses include without limitation:

   - Libel
   - Privacy
   - Copyright
   - Trademark

- Obscenity and child pornography
- Electronic Communications Privacy Act
- Digital Millennium Copyright Act
- Technology, Education and Copyright Harmonization Act
- Computer Fraud and Abuse Act, which prohibits “hacking”, “cracking”, and similar activities
- Applicable export control statutes, regulations and contractual provisions
- The University’s code of student conduct
- The University’s non-discrimination policies
- All applicable software licenses
- Applicable laws and policies of other states or countries or on other systems or networks.

c. **Compliance with copyright laws** - Authorized Users may not copy, distribute, modify, or display another’s work unless the copyright owner has given permission to do so; it is in the “public domain”; doing so would constitute “fair use”; or an “implied license” to do so was granted. Using Resources to download or share copyrighted music, movies, television shows or games without the permission of the copyright owner may result in sanctions.

d. **Avoidance of harassment** - No member of the community may use Resources to libel, slander, or harass any other person.

Harassment includes, without limitation, the following:

(1) Intentionally using Resources to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or others;

(2) Intentionally using Resources to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;

(3) Intentionally using Resources to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease;

(4) Intentionally using Resources to disrupt or damage the academic, research, administrative, or related pursuits of another;

(5) Intentionally using Resources to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

e. **Responsible use of Resources** - Authorized Users are responsible for knowing what Resources are available, remembering that the members of the community share them, and refraining from all acts that corrupt, interfere, waste or prevent others from using these Resources, or from using them in ways that have been proscribed by the University and by federal, Michigan and all other applicable laws.

f. **Preserving information integrity** - Authorized Users are responsible for awareness of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to verify the integrity and completeness of information compiled or used. When information or communications appear to be contrary to expectations, one should verify the correctness of the data or message with the person believed to have originated it.

g. **Use of personal computing systems or devices** - Authorized Users are responsible for the security and integrity of information stored on Resources, including hardware and software. Particular care must be taken when using portable laptop or storage devices. This responsibility includes:

- Making regular backups
- Protecting backup media
- Safeguarding any portable media, such as laptops and thumb-drives
- Not storing passwords or other account access information
- Protecting Confidential Data (as defined in OU AP&P #860 Information Security) by use of encryption, password protection or other strategies
- Controlling physical and network access

- Installing and using operating system patches, virus protection, firewalls and other protective tools.

III. ACCESS TO RESOURCES

Access - An Authorized User must be specifically authorized to use particular Resources by the campus unit responsible for operating the Resources. Divisional leaders, departmental managers, Data Stewards designated in OU AP&P #860 Information Security, and systems administrators are authorized to inspect, use or assign for use Resources in their area of responsibility.

Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. No third-party access to any accounts with access to Resources is permitted without advance, written authorization from the Office of Legal Affairs. An Authorized User is responsible for any use of the individual account. Authorized Users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users.

Use of privileged access - Special access to information or other special computing, network or information technology privileges or job responsibilities are to be used in performance of official duties only. Information obtained through special privileges is to be treated as confidential, except as otherwise provided in any University policy, procedure or ordinance or as required or permitted by applicable law.

Termination of access - When an Authorized User ceases to be a member of the campus community through graduation, failure to enroll, change of guest status or termination of employment, or if an employee is assigned a new position and/or responsibilities within the University, access and authorization must be reviewed and may be terminated immediately in the University's sole and exclusive discretion. An individual must not use facilities, accounts, access codes, privileges, or information without authorization appropriate to the new situation.

Attempts to circumvent security - Authorized Users are prohibited from attempting to circumvent or subvert any security measures. The Chief Information Officer must authorize use of computer programs, processes or devices that intercept or decode passwords or similar access control information. Authorized Users may not obtain unauthorized Resources, deprive another Authorized User of Resources, or gain unauthorized access to Resources by using knowledge of an unauthorized password or loophole in a computer security system.

Denial of service and other harmful activities - Deliberate attempts to degrade the performance of Resources, or to deprive Authorized Users use of or access to Resources, is prohibited. Harmful activities that are prohibited include without limitation: creating or propagating viruses; disrupting services; damaging files; intentional destruction or damage to Resources.

Monitoring and inspection of logs and files - The University seeks to maintain a secure computing system, but cannot and does not guarantee security or confidentiality. In addition to accidental and intentional breaches of security, the University may be compelled to disclose electronic information as required by law.

As part of necessary routine operations, Oakland University occasionally gains access to Resources. Suspected policy violations discovered during such routine operations will be reported as noted in the Procedures and Sanctions section. All other information accessed during such routine operations will be treated as confidential, except as otherwise provided in any University policy, procedure or ordinance or as required or permitted by applicable law.

When the University has a good faith belief of suspected violations of this policy or unlawful activity, it may access Resources necessary to investigate such suspected violations.

The University may access Resources and/or accounts for any other reason as permitted or required by law.

For accounts granted to University employees, and for University-owned or-administered computers they use, the employee's department head, may, based on a good faith belief that such action is necessary to respond to an operational or administrative problem or to investigate suspected violations of University policy or unlawful activity, request access to the employee's Resources.

If required by law or this policy, the Authorized User will be notified that his/her Resources have been accessed.

Using Resources for unauthorized monitoring is prohibited.

Academic dishonesty - Use of Resources in accordance with the high ethical standards of the University community is required. Academic dishonesty (plagiarism, cheating) is a violation of those standards.

Use of copyrighted information and materials - Using, inspecting, copying, transmitting, sharing or storing copyrighted software programs, music, movies, television shows or other material in violation of copyright is prohibited.

Use of licensed software - No software may be installed, copied, or used on Resources except as permitted by the owner of the software. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly followed.

E-mail - By opening and using your e-mail account, Authorized Users agree and consent that the University may access the account for administrative and all other

purposes permitted or required by law and/or the University's policies, procedures and ordinances, which may require the University or its e-mail provider (if applicable) to access and disclose to the University any information stored within the account. The University does not centrally retain or archive e-mail sent, processed or received by the University e-mail system. E-mail may be retained, stored or archived by external providers of e-mail services.

Web sites, blogs, political campaigning, commercial advertising, sponsorships and other public information uses - The use of Resources in political campaigns or for commercial purposes is prohibited unless authorized by the President of the University. Web sites displaying sponsorships require special attention; corporate logos or sponsored links require technical guidelines approval through standards available from the University's Communications and Marketing office. All official university web site development on the oakland.edu domain must meet the technical guidelines standard.

Game playing, web surfing and other recreational activities - Limited recreational game playing, web surfing or other recreational activity that is not part of an authorized and assigned research or instructional activity is tolerated (within the parameters of each department's or division's rules). Resources are not to be used for excessive recreation, as determined by the University in its sole and exclusive discretion, outside residential and recreational areas. Individuals engaged in recreational activities while occupying a seat in a public computing facility must give up that seat when others who need to use the facility for academic or research purposes are waiting.

Unrelated business - Resources may not be used in connection with compensated outside work, business unrelated to the University, or for the benefit of organizations not related to the University except in connection with scholarly pursuits (such as faculty publishing activities or work for professional societies) or other activities authorized by the President of the University. This and any other incidental use must not interfere with other users' access to Resources and must not be excessive. State law restricts the use of State facilities for personal gain or benefit.

Prurient interest - Use of Resources must not violate any federal, Michigan or any other applicable laws. To the average person, applying contemporary community standards, the dominant theme of any electronic resource taken as a whole shall not appeal to the prurient interest, such as does pornography.

Issues of Safety and well-being - The University may suspend an individual's access to and use of Resources for reasons relating to his/her physical or emotional safety and well-being, or for reasons relating to the safety and well- being of others, or the safety and well-being of University property. Access will be promptly restored when safety and well-being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action.

Investigative contact - If contacted by a representative from an external organization/(FBI, Homeland Security, police department, etc.) or a representative from an internal investigating body conducting an investigation of an alleged violation involving Resources, inform the Office of Legal Affairs immediately. Refer the requesting agency to the Office of Legal Affairs; that office will provide guidance regarding the appropriate actions to be taken.

Reporting security and abuse incidents - Report any discovered unauthorized access attempts or other improper usage of Resources to University Technology Services (uts@oakland.edu) or as noted in the Desktop Emergency Guide under Information Technology Compromises.

IV. SANCTIONS

Imposition of sanctions - The University may, in its sole and exclusive discretion, impose sanctions and/or disciplinary action for violations of this policy including without limitation the sanctions described in this policy.

Sanctions - In all cases of an actual or suspected violation of this policy, access to Resources will be suspended until final resolution as noted below.

1. Student Violations

   i. First and minor incident

   If a student violates this policy, and (1) the violation is deemed minor by a representative of University Technology Services in his or her sole and exclusive discretion, and (2) the student has not been implicated in prior incidents, then the incident may be dealt with by a representative of University Technology Services. The alleged offender will be furnished a copy of this document and will sign a letter agreeing to conform to the policy to be kept by University Technology Services.

   ii. Subsequent and/or major violations

   Subsequent and/or major violations, as determined by a representative of University Technology Services in his or her sole and exclusive discretion, will be forwarded to Dean of Students and Office of Legal Affairs.

   iii. First and minor incidents and subsequent and/or major violations - Students in the School of Medicine

   Any violations of this policy, as determined by a representative of University Technology Services in his or her sole and exclusive discretion, will be forwarded to School of Medicine Associate Dean for Student Affairs and Office of Legal Affairs.

2. Employee Violations

   Reports of violations will be forwarded as based upon the alleged offender's relationship to the University. University Technology Services will first seek to educate those found to be in violation of this policy

   i. University Employees – Staff violations will be forwarded to Human Resources, the employee's supervisor, and Office of Legal Affairs.

   ii. University Employees – Faculty violations will be forwarded to the Office of the Provost and Office of Legal Affairs.

3. Violations by other Authorized Users

   i. First and minor incident - If other Authorized Users violate this policy, and (1) the violation is deemed minor by a representative of University Technology Services in his or her sole and exclusive discretion, and (2) the Authorized User has not been implicated in prior incidents, then the incident may be dealt with by a representative of University Technology Services. The alleged offender will be furnished a copy of this document and will sign a letter agreeing to conform to the policy to be kept by University Technology Services.

4. Subsequent and/or major violations

   Subsequent and/or major violations, as determined by a representative of University Technology Services in his or her sole and exclusive discretion, will be forwarded to the Office of Legal Affairs.

Range of disciplinary sanctions - Persons in violation of this policy are subject to the full range of sanctions, including without limitation the loss of access privileges to Resources, disciplinary action, dismissal from the University, and legal action. Some violations may constitute criminal offenses, as outlined by federal, Michigan and all other applicable laws; the University will carry out its responsibility to report such violations to the appropriate authorities.

Appeals - Appeals should be directed through the already-existing procedures established for employees and students. Other Authorized Users may appeal to the Office of Legal Affairs.

RELATED POLICIES AND FORMS:

Merit Network, Inc., operates the statewide network MichNet, which provides Internet access for the University. Merit is a non-profit corporation governed by all

thirteen of Michigan’s four-year publicly supported universities, including OU. University participation in MichNet and access to the Internet in general is governed by their Acceptable Use Policies.

OU AP&P #860 Information Security

APPENDIX: