EASTERN MICHIGAN UNIVERSITY DIVISION of INFORMATION TECHNOLOGY	Policy	
	Effective Date	**Date of Last Revision**
	March 18, 2014	October 15, 2014

Chapter Name	
Computer Use	
Chapter Number	**Title**
3.1	**Acceptable Use of Information Technology Resources**

1.0 Purpose

The University provides information technology (IT) resources to students, faculty, and staff. All users have the responsibility to use these resources in an effective, efficient, ethical, and legal manner. Appropriate and responsible use stipulates that EMU IT resources be used in a manner consistent with the University's instructional, public service, research, and administrative objectives and all local, state, and federal laws. All uses inconsistent with these objectives are considered to be inappropriate use and may jeopardize further access to services and lead to disciplinary action, up to and including discharge.

2.0 Scope

Anyone using or accessing EMU computers, networks, systems or data is subject to the provisions of this policy. EMU faculty, staff, emeritus faculty and staff, registered students, alumni, and approved guests are permitted to use EMU’s computing and networking services, but are subject to the terms of this policy during that use. Individuals who use personally-owned equipment while connected to the university network are subject to the provisions of this policy while connected to the network. Use of EMU’s computing and networking facilities and equipment by unauthorized persons is prohibited.

3.0 Policy

Information technology resources are provided by Eastern Michigan University (EMU) to all university employees in support of the University's mission. The University provides IT resources with the stipulation that users contribute to creating and maintaining an open community of responsible users through the ethical and responsible use of University-provided computing resources. All uses inconsistent with these objectives are considered to be inappropriate use.

A. Academic Freedom

Eastern Michigan University endorses the principle of Academic Freedom – the freedom to discuss academic subjects fully, freedom to engage in research and to publish the results of research, and freedom to write or speak as citizens without fear of institutional censorship or discipline, provided individuals do not represent themselves as speaking for the University. Policies concerning Information Technology (IT) will be administered with full respect for the principle of Academic Freedom.

Further, EMU understands the importance of securing the confidentiality of research data and other academic materials. In a networked electronic environment, it is not within the means of the University to provide absolute assurances of confidentiality with respect to data stored on EMU equipment. Faculty members, particularly, are encouraged to seek training and advice from IT that will empower them to protect confidential information related to their academic work.

B. Appropriate and Responsible Use

Appropriate and responsible use stipulates that EMU’s computing resources be used in a manner consistent with the University's instructional, public service, research, and administrative objectives. Use should also be consistent with the specific objectives of projects or tasks for which use was authorized. All uses inconsistent with these objectives, as modified by subsection D, Personal Use of EMU IT Resources, are considered to be inappropriate use and may jeopardize further access to services.

In brief, employees of EMU may not:

1. Assume another person's identity or role through deception or without proper authorization.
2. Communicate or act under the guise, name, identification, email address, signature, or indicia of another person without proper authorization.
3. Communicate under the guise of an organization, entity, or unit that you do not have the authority to represent.

The University characterizes as unethical and unacceptable any activity through which an individual:

1. Violates such matters as University or third party copyright or patent protection and authorizations, as well as license agreements and other contracts.
2. Interferes with the intended use of the information resources.
3. Seeks to gain or gains unauthorized access to information resources.
4. Without authorization, destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of computer-based information and/or information resources.
5. Without authorization invades the privacy of individuals or entities that are creators, authors, or users of information resources.

C. User Responsibilities

By using the University's computing services, you accept the following responsibilities.

1. Respect the Rights and Privacy of Other Users

   For example, employees of EMU may not:

   - Intentionally seek information on, obtain copies of, or modify any e-mails, files, or passwords belonging to other users or the University.
   - Represent others, unless authorized to do so explicitly by those users.

2. Respect the Rights of the University
   Information technology resources, systems, and services are the property of EMU. These include all components of the electronic communications, physical infrastructure, and any electronic communications address, number, account, or other identifiers associated with the University.

   a. The University reserves the right to inspect, monitor and/or disclose electronic files, records, and communications in transit or storage only in the following circumstances:

      - When required by compliance with a court order (i.e., search warrant) or compliance with Federal or state law (i.e., subpoenas).
      - When required by the University's legal office to comply with a documented Freedom of Information Request.
      - When there is a written allegation filed with the appropriate legal or personnel office of the University stating that there has been a violation of University policy, rule, regulation, or procedure and that a formal due process hearing has been conducted with the employee who is the subject of the allegation
      - To maintain the security or performance of the computer network infrastructure.
      - Those instances in which an employee is absent from work and access to specific computer records is critical to continue the work of the University during their absence.

   b. In these specific circumstances, the files, records, and communications to be inspected, monitored, or disclosed must be explicitly listed in the authorizing document provided to the Chief Information Officer or his/her designee.

   c. EMU reserves the right to withdraw information technology resources, systems, or services from anyone who misuses the system.

3. Respect the Legal Protection Provided by Copyright and Licensing of Programs and Electronic Media

Users are expected to obey copyright laws. Copyright protected materials include, but are not limited to, software, music, written works, audio and videos, photographs, and electronic books (e-books). Do not use your computer or other electronic device in a manner inconsistent with or in violation of EMU Board Policy 4.4 regarding copyrights.

For example, employees of EMU may not:

- Use file-sharing programs to obtain copyrighted material such as music, DVDs, and other protected items without permission of the copyright holder
- Make copies of a licensed computer program to avoid paying additional license fees or to share with other users.

4. Respect the Intended Usage of Resources

You are responsible for all activity on your account conducted by you. You are responsible for all authorized activity on your account conducted by users you have authorized. You are not responsible for activity resulting from the unauthorized or illegal capture of your access credentials.

For example, employees of EMU may:

- Use only those resources assigned to you by authorized system administrators for the purposes specified.
- Not access, use, or divulge such resources unless explicitly authorized to do so by the appropriate authority.
- Not use University resources assigned to you or others for profit-making or fund-raising activities unless explicitly authorized to do so by the appropriate authority.
- Not use University resources to support or oppose a candidate or the qualification, defeat, or passage of a ballot proposal (per Michigan Campaign Finance Act, Act 388 of 1976).
- May not advertise or solicit for commercial events or endeavors in a manner inconsistent with or in violation of EMU Board Policies 14.7 and 14.8 regarding commercial sales.

5. Respect the Intended Usage of Systems for Electronic Exchange

All University electronic communications are to be used in an ethical and responsible manner. Do not send or publish threatening or harassing communications. Do not falsify or forge authentication, e-mail headers or other postings.

Examples of inappropriate use of communication resources include:

- Soliciting e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding spam or e-mail service inhibitors (intentional e-mail transmissions that disrupt normal e-mail service).
- Sending "chain mail" or e-mails repeatedly that misuses or disrupts resources.
- Creating or intentionally sending viruses or other harmful programs or files.

For example, employees of EMU may not:

- Indiscriminately send unsolicited mass e-mail unrelated to the University's academic or business initiatives.
- Send forged e-mail, e-mail that threatens or harasses other users, unsolicited mass e-mail not related to the purpose of the addressed group(s), or promotional e-mail for commercial or profit-making purposes.

6. Respect the Integrity of the System or Network

It is your responsibility to use effective passwords and to safeguard those passwords. You are also responsible for the physical security of information technology devices you use and the data they contain. The Division of IT's website provides instructions for creating effective passwords that are easy for users to remember but are difficult to decipher or "crack".

Do not try to access a computer, the EMU system, or other devices without appropriate permission and without following proper login procedures.

Avoid activities that jeopardize the continued function of the university's computer network or that prevent other users from using the university's computer network or accessing their assigned network resources.

Example:
EMU employees may not intentionally develop or use programs, transactions, data, or processes that harass other users, infiltrate the university's network, or damage or alter the software or data components of an attached computer system. This would not apply to academic programs that have worked with the Division of IT to establish a closed network system for educational or research purposes.

7. Adhere to All Legal Statutes and University Policies
Users of EMU information technology resources agree to comply with applicable federal and state laws and the policies, standards, and procedures of the University. Do not use University-provided computing resources to do something illegal, threatening, or deliberately destructive or harmful.

D. Personal Use of EMU IT Resources

EMU employees may use the University information technology resources for incidental personal purposes provided such use does not:

- Directly or indirectly interfere with the University operations and services.
- Burden the University with noticeable incremental cost.
- Interfere with the user's employment or other obligations to the University.
- Violate the law, University policies or procedures, or reasonable standards of decency and civility.

Guidelines on how to save and protect employee-owned personal files on university-owned computers is documented in EMU IT Procedure 7.3.P.2, "Personal and Private Folder".

E. Reporting an Incident

If an incident is a threat to personal safety, contact Campus Police at the Department of Public Safety.

To report an incident involving the misuse of Information Technology resources, contact the Chief Information Officer (CIO) or the IT Security Office via email, letter, or telephone.

When an incident is reported, the CIO, IT Security Office and/or the Campus Police may (as needed and appropriate) consult with the Office of the President, the Office of Legal Affairs, Staff and Academic Human Resources Offices, and other University Offices/Departments.

4.0 Responsibility for Implementation

The authority for this policy is Eastern Michigan University policy 15.2 "Information Technology Security and Confidentiality". The University's Chief Information Officer is responsible for the implementation of this policy.

5.0 Enforcement

Any employee found to violate federal or State of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under University policy. Any student found to violate federal or State of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under EMU's Student Code of Conduct. Any suspected violation of State or Federal laws will be reported to the appropriate legal authority for investigation.

The University reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other action.