Westfield State University
Policy concerning:

APPROVED: June 2015 REVIEWED: June 2024

SOFTWARE AND HARDWARE ACQUISITION AND USAGE

PURPOSE

The purpose of this policy is to provide compatibility and control of software and hardware utilized at the University. This policy shall be enforced in conformity with all applicable local, state, and federal regulations and laws.

SCOPE

This policy applies to all students, faculty, staff, volunteers, vendors, consultants, contractors, or others (herein afterwards referred to as "constituents") who use or have authorized access to University Information Technology Resources. This policy is supplemented by the policies of those networks to which the University is interconnected, including, but not limited to, the University of Massachusetts Information Technology Systems group, the Commonwealth of Massachusetts' Information Technology Division, UMass Online, etc. It covers all University information whether in hardcopy or electronic form and any systems which access, process, or have custody of business data. This policy also applies to all information, in any form and in any medium, network, internet, intranet, computing environments, as well as the creation, communication, distribution, storage and disposal of information.

For the purposes of this policy, "Information Technology Resources" means all computer and communication facilities, services, data, and equipment that are owned, managed, maintained, leased or otherwise provided by the University. Information Technology Services (ITS) refers to authorized personnel currently assigned to Infrastructure Services and Administrative Systems. Area Security Officials shall be the supervisor of each department or program with the authority to grant access to Information Technology Resources. The Information Technology Resource Hardware and Software Review Committee refers to members of the Security Policy Committee that will ensure compatibility, functionality, and feasibility in order that the request meets the needs of the business operation it is intended to support. This includes, but is not limited to, ensuring that hardware and software does not currently exist to meet the needs of the business operation.

The use of the University's Information Technology Resources constitutes an understanding of, and agreement to abide by, this policy. Additionally, all constituents must protect and if necessary, intervene to assure that others protect the confidentiality, integrity and security of all Information Technology Resources.

USER OWNERSHIP AND RESPONSIBILITIES

It is the responsibility of any person using the University's Information Technology Resources to read, understand and follow this policy. In addition, all users are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of Information Technology Resources. Any person with questions regarding the application or

meaning of this policy should seek clarification from their ASO or from the Information Security Officer. The University owns and maintains the information stored in its Information Technology Resources and it limits access to its Information Technology Resources to authorized users. Users of Information Technology Resources have a responsibility to properly use and protect these resources, respect the rights of other users, and behave in a manner consistent with any local, state and federal laws and regulations, as well as all University policies. Information Technology Resources, including Internet bandwidth, are shared among the community and users must utilize these resources with this understanding.

Users must respect all intellectual property rights, including any licensing agreements applicable to information and resources made available by the University to its community.

Information Technology Resources are provided to support the mission of teaching and learning and to conduct official University business. Therefore, the University bears no responsibility for the loss of any personal data or files stored or located on any system.

The University does not systematically monitor communications or files. Users must be aware of, and responsible for, material which community members may post, send, or publish using its network, servers and other resources including the internet.

PROCEDURES

A list of currently approved software and hardware is available by contacting AISSD or the Chief Information Security Officer.

1. Software and Hardware Acquisition

    a) Requests for software and hardware must have the approval of the Information Technology Resource Hardware and Software Review Committee, including, but not limited to, the future support of the software and/or hardware.

    b) Software and hardware, including those that are externally hosted, are required to follow this acquisition and usage process, even if it is at no cost.

    c) Purchase or installation of any software or hardware that has not been approved by the Information Technology Resource Hardware and Software Review Committee is strictly prohibited.

    d) After approval, it is the responsibility of the requestor to:

        1. Have the funds available in their appropriate budget including a future financial plan.

        2. Coordinate with the Information Technology Resource Hardware and Software Review Committee to ensure dependencies for the future operations of the software and/or hardware.

e) All requests for software and hardware acquisition must follow the approved University Procurement Process policy (Administrative Policy #320) and be in compliance with all local, state, and federal laws and regulations, as well as any other applicable University policies.

f) The University shall honor and respect all software copyright(s) and adhere to the terms of all software licenses to which the University is a part of:

1. Software, hardware, and its associated documentation may not be duplicated for use on University Information Technology Resources or elsewhere unless expressly authorized by fair use or agreement.

2. Software and/or hardware may be utilized on local area networks or multiple machines in accordance with applicable licensing agreements.

g) This policy is also inclusive of software as a service (SaaS).

2. Software and Hardware Installation and Maintenance:

a) All hardware and software assets, regardless of the funding source, remain the property of the University and must be in compliance with The Fixed Assets, Capitalization, and Inventory Control Policy (Administrative Policy # 601).

b) University Information Technology Resources must be kept both virus and malware free and in compliance with licensing agreements.

c) All installations of approved software and/or hardware must be coordinated through the appropriate Information Technology Department.

d) Generally, the purchase of a single copy of any software entitles the owner to use the software on one (1) device.

e) Before installing any approved University software on any home or personal machines, please check with the Technology Support Services department (TSS).

f) Installation of any software or hardware not approved is strictly prohibited. Any unapproved software and/or hardware found to be installed on University Information Technology Resources shall be considered a security incident and shall be reported and acted upon in accordance with the Information Security Incident Response Policy.

g) Software and hardware may be purchased with maintenance and upgrade options. Unless otherwise agreed upon by the appropriate Information Technology Department, the requestor is responsible for budgeting for any and all future maintenance and upgrade costs.

3. Server related software and hardware shall follow the same procedures and be approved by the Director of Administrative Systems and/or the Director of Infrastructure Services and be in compliance with all University polices and its procedures and guidelines.

4. Computer Lab software and/or hardware shall follow the same procedures and is managed by the TSS and utilizes Deep Freeze to restore the image to original configuration on log off or restart.

5. Any exceptions to this policy must be approved in writing by the Chief Information Security Officer.

6. Failure to comply with these guidelines and their supporting policies may be subject to disciplinary action.

REVIEW

This policy shall be reviewed annually by the Chief Information Security Officer and the Director of Technology Support Services.