REMOTE ACCESS

PURPOSE

The purpose of this policy is to define the requirements for connecting to the Westfield State University network from any remote system. These requirements are designed to minimize the potential exposure to damages, which may result from unauthorized use of University resources. Damages include the breach of confidential, sensitive, or organizational information and intellectual property, damage to public image, damage to critical internal systems, the compromise of system availability, or the corruption of information integrity.

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 any and 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. Academic Technology Services Support Desk (ATSSD) refers to authorized personnel currently assigned to Support Desk under Academic Information Services. Area Security Officials shall be the supervisor of each department or program with the authority to grant access to Information Technology Resources.

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 his or her supervisor, 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 all communications or files. Users must be aware of, and responsible for, material which they send or publish using its network, servers, and other resources, including the Internet.

PROCEDURES

1. All remote access to University applications, systems and hardware shall be authorized and approved through Information Technology Services.

2. Any access not explicitly authorized and approved is forbidden.

3. Remote access to specific applications, systems, components and technology infrastructure shall only be granted to users with a legitimate business need.

4. The level of access granted and privileges assigned shall be limited to the minimum required to perform assigned duties.

5. Employees and third parties authorized to utilize remote connections shall ensure that unauthorized users are not allowed access to the University internal network utilizing these connections.

6. All individuals and machines, while accessing the network, including company-owned and personal equipment, are considered an extension of the University 's network.

7. All devices, including personally-owned computers, that are connected to the network via remote access technologies must;

    i. Employ up-to-date anti-virus software, and be up-to-date on available patches,

    ii. Employ security patches for installed operating systems (with auto-update, enabled), web browsers, and common applications shall be applied,

    iii. A firewall must be enabled on each applicable device.

8. Remote access may only be used to conduct business-related work. Personal, private, or commercial use of any service available remotely is not permitted.

9. Users agree to protect University information assets from unauthorized access, viewing, disclosure, alteration, loss, damage, or destruction.

10. Remote access to data or services may not be used to copy private or personal information, such as that residing on a privately owned computer, to company file shares, or other University owned information systems.

11. Remote access to data or services may not be used to store University information on a personal system, file share or other non-University owned system without prior approval from the Chief Information Security Officer.

12. Any constituent found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including termination of access or employment (if applicable).

REVIEW

This policy shall be reviewed annually by the Vice President of Administration and Finance and the Chief Information Security Officer.