

**UMB, UMMC, UPI and SOM Enterprise  
Campus Remote Access  
Draft Policy #2  
Jan-2005**

**Executive Summary**

Members of the campus community and others may require access to networked resources to conduct enterprise mission-related work from home, hotel rooms or off-campus offices. Providing secure remote access makes enterprise computing and information resources available well beyond the physical borders of campus. This greatly expands the universe of threats and risks to which network resources are exposed. Certain extra measures are required to protect enterprises resources under these conditions.

**Goal**

The purpose of this policy is to set standards for connecting to UMB, UMMC, UPI or SoM networks from remotely situated workstations or devices. These standards are intended to minimize the risk of network disruption and loss or disclosure of sensitive information such as intellectual property, personnel data or patient information.

**Scope**

This policy applies to the enterprise workforce (i.e., faculty, staff and students) as well as to vendors, contractors and others who seek access to enterprise or individual computer resources.

**Definitions**

Departmental IT Manager – Individual or group responsible for maintaining network devices for an organization and/or department.

Dual Homing – Having simultaneous connections to more than one network from one workstation or device. Examples include, having a wireless cards connecting to the SoM network and a wired network card connecting the UMMS network or using a dial-up connection to AOL while connected via a VPN to the enterprise.

Remote Access – Secure access to the enterprise network or its resources through networks, devices or media not directly controlled by this enterprise. Web-based services are not subject to the guidelines established for secure remote access.

Split Tunneling – Establishing simultaneous virtual “tunnels” to two different networks using VPN software.

**General Policy**

Remote access is a privilege granted to certain individuals who have a demonstrated need to perform mission-specific activities using enterprise resources while situated off campus. It may not be possible for everyone to receive the privilege of remote access. A person’s request for remote access to information systems that contain sensitive data must be documented in writing and authorized by his or her supervisor.

Remote access is a de facto extension of the enterprise network. Remote workstations and devices must provide as much security for the enterprise and its information resources as is provided through on-campus workstations and devices. All enterprise acceptable use and security policies that apply to access from on-campus workstations also apply to remotely connecting workstations. In particular,

- Remote access must be strictly controlled through the same on-campus authentication and authorization measures. Logon information may not be shared with others. Unauthorized people (including family and friends) are not allowed to use enterprise resources.
- Workstations owned by workforce members, contractors or other affiliates of the enterprise must comply with the Enterprise Operating System Patch Management and Anti-Virus policies.
- Data transmitted between remotely situated workstations and the network must be encrypted (128-bit minimum length). Acceptable mechanisms of encryption include either institutionally approved VPN or browser-based SSL connections.
- Points for remote access entry into enterprise networks must be configured to drop inactive connections after 30 minutes whenever possible. Using contrivances to circumvent this requirement is prohibited.
- Third-party products or services (e.g., PCAnywhere, VNC, GoToMyPC, etc.) that establish remote access or that bypass institutionally approved VPN or browser-based SSL connections may not be used unless explicitly approved by local network administrators. Third-party product access will be controlled by blocking known ports at local firewalls.
- PC modems or PC fax connections to telephone equipment are not permitted without the explicit knowledge and approval of the departmental IT manager.

### **Guidelines**

- Because they permit unregulated interconnections between two or more networks, split tunneling and dual homing should not be used.
- Remote users should log off from their remote connection when they leave the computer to prevent inadvertent network access by others.
- Whenever it is feasible, remote access workstations should employ a personal firewall (software- or hardware-based).

### **Auditing and Monitoring**

Information technology staff will routinely monitor logs of remote access activity and inspect network traffic for evidence of compliance with this policy. Access may be revoked at any time without notice.

### **Effective Date**

The rules defined in this document are effective immediately.

**Violations**

Failure to follow these principles is a violation of this policy.

It is the responsibility of each departmental IT manager to make sure that they are keeping their departmental systems in compliance with the above stated policy. Failure to do so constitutes a violation of policy.

**Enforcement**

Violations in policy will result in progressive disciplinary action dealt with through normal disciplinary processes within each organization.

**Revisions**

This policy will be reviewed and revised as needed.