


Name of Policy: Remote access security.		 Original effective date: January 29, 2009	
Policy Number: 3364-65-11			
Approving Officer: President			
Responsible Agent: Vice President of Information Technology			
Scope: all University of Toledo campuses			
X	New policy proposal	<input type="checkbox"/>	Minor/technical revision of existing policy
<input type="checkbox"/>	Major revision of existing policy	<input type="checkbox"/>	Reaffirmation of existing policy

(A) Policy statement

Remote access capability via virtual private network (VPN) as provided by the university information technology will be the only method of obtaining remote access to university computing assets located on the internal campus network.

(B) Purpose

This policy requires the use of university provided VPN capabilities as the only method of remote access to computing systems residing on the university's internal network.

Remote computer access is a popular method of accomplishing work away from the office, while at home, or while traveling. However, remote access capabilities can add security vulnerabilities because such services increase the number of access points that hackers can use to gain entry. It is critical that these access points be properly secured.

Because many university organizations now permit the business use of computers that are not owned by the university, the network perimeter has been extended to include those computers. However, it should not be implied that this policy requires organizations to be responsible for the installation, maintenance and support of computers and personal digital assistants that are not owned by the university.

(C) Scope

The scope of this information technology policy includes university computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the university who use and administer such systems.

This remote access policy does not apply to access to web enabled systems provided by the university and designed for use and access from off campus (e.g. www.utoledo.edu, myut.utoledo.edu, email.utoledo.edu, files.utoledo.edu, etc.)

(D) Procedure

Virtual Private Network (VPN) as provided by the information technology is the only method of obtaining remote access to internal university computing assets.

- (1) Authorization. Authorization for VPN remote access authorization can be requested by university faculty and staff through the online VPN request process located on information technology's web page. VPN authorization requires a supervisor's approval.

Authorization for VPN access for vendors or external organizations will be processed through the IT help desk, 419-530-2400. Vendor access must have a sponsoring university manager's approval and justification.

- (a) VPN authorization is based on business justification and may not be granted if external means of access exist. Examples of alternative means include:
 - (i) Clinical Portal – alternative is <http://cp.utoledo.edu>
 - (ii) Exchange email – alternative is <http://email.utoledo.edu>
 - (iii) Personal/dept file share drive – alternative is <http://files.utoledo.edu>
 - (iv) Remedy/Help Desk – alternative is <http://tech.utoledo.edu>

- (2) Authentication. Authorized VPN users will be authenticated via UTAD credentials.
- (3) Responsible use. VPN users must adhere to university policy on the responsible use and agree to keep remote computing systems up to date with critical operating system security patches and anti-virus protection.
- (4) Remote connections. Users shall not establish a separate internet connection while simultaneously connected to the university network through the use of multiple network cards, modems or other routing and bridging techniques.
- (5) Records. Information technology shall establish and implement a procedure for keeping their directories of approved users and dial-in numbers accurate, current and protected.
- (6) Auditing. Audit logs will be regularly examined and comply with the security auditing requirements addressed in The University of Toledo, "Information Security Framework."

<p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>January 29, 2009</u> Date</p> <p>Review/Revision Completed by: Vice President of Information Technology</p>	<p>Policies Superseded by This Policy:</p> <p>None</p> <p>Initial effective date: January 29, 2009</p> <p>Review/Revision Date: Next review date: January 29, 2012</p>
---	--