

Remote Access Security Standard

Information Technology Security Standard #4, v2.1

Standards Name: Remote Access Security Standard

Original Release Date: 5/26/2005

Latest Revision Date: 10/19/2007

Authority: This standard was approved by the Information Security Council, acting as representatives of the CIO and the Technology Leadership Committee (TLC). It derives its authority from the CIO and the campus Information Technology (IT) community.

Summary and Scope: This standard provides the security requirements for all SU employees who are manipulating/accessing University Data classified as “Enterprise” or “Confidential” from remote locations. These are referred to as “Remote Workers” or “Remote Users.” It also covers the transport of such data via mobile devices, including laptops, PDA’s, smartphones, flash drives, CD’s/DVD’s, and other removable media.

The detailed explanation for classifying such University Data is found in the Syracuse University Information Security Standard. The Desktop Security Standard provides requirements for mobile devices, such as laptops and PDA’s, and the Encryption Standard provides requirements for all removable media and summarizes the various encryption requirements across all device types.. In essence, the Remote Access Standard is a framework for other security standards and procedures that apply in situations where University Data is exiting the University-run IT systems.

Recognizing that there are some common data sets that are frequently accessed remotely or transported for which these requirements can become onerous and not in the overall interest of the University, the Information Security Standard provides further guidance on when exceptions are permitted.

The standard does not apply to people handling other data sets, such as their own personal data (some of which fits within the idea of the Myslice “self service” data) or simply viewing public University Data, but note that certain campus systems and services are only available when remote access technologies such as the VPN are used.

Responsible Office: ITS/CIO.

Requirements and Practices for all Remote Users

1. **Remote Access** (applies to all devices that are Internet-aware, e.g., that have e-mail capability, instant messaging, web browsers, etc.)

The desktop/laptop security standard defines the following as required on any laptop or PC used for working remotely:

- Antivirus software that is pulling daily updates.
- All security patches for Windows, web browsers, and common applications are applied in a timely manner.

Additional requirements exist for remote work:

- The machine/device can be trusted. This means that the machine must be built and maintained by a professional IT organization, or by the user in a manner that creates confidence in the security of the machine. Home machines used for remote work should never be used with applications prone to malware infections, such as peer-to-peer, gaming, and free (and untrusted) software downloads. *The use of web kiosks and other untrusted machines for accessing any form of University Enterprise/Confidential Data or for entering a campus NetID/password or other SU-related credentials violates this standard and is an extremely dangerous practice. Never trust public machines.*
- The user is approved by the unit/department to work remotely. Approval for remote access follows the procedure at <http://its/security/remotearchive/authprocess.cfm>. Use of smartphones and pda's to access e-mail and other campus resources remotely also requires approval. Many of the same risks found with PC's apply to these devices.
- All reasonable efforts are made to protect University Data, keeping it "in house" on secured servers and devices wherever possible.

The final requirement can be achieved in various ways, and each user must employ the appropriate methods for accessing University Data. Such Remote Access from mobile or home PC's can generally be performed through one of three common approaches to remote work, listed here by increasing access rights and increasing security requirements:

- If the user really only needs to access e-mail or other public web services, then no additional requirements exist. Direct access from the remote PC is acceptable. This assumes the e-mail system provides an encrypted network path and secure storage of messages.
- If the user has a limited need to use enterprise applications, they may be able to work via a Terminal Server provided by ITS or the department. Again, no additional requirements exist on the remote machine for these users, but the

department must take precautions so that users will not download sensitive files to their remote machine.

- For users needing access to their desktop machines or who need wider access to campus resources, the user must use the campus VPN service. In most cases they will “Remote Desktop” into their office machine and run most applications from that machine. Other acceptable access technologies include SSH, pcAnywhere, VNC, and Timbuktu. External, hosted remote access tools such as GotoMyPC are not acceptable.

2. Transporting University Data via laptops, PDA’s, and other media is a question of whether encryption is required: the Information Security Standard and Encryption Standard can answer those questions. Removable media are a particular risk, due to the ease with which they can be lost or stolen. The authorization process used for Remote Access does not apply to removable media but units should formulate policies about employees taking media from the office and discourage the practice.