

Computing Resource Security Policy

A great deal of important and sensitive data now resides on computers throughout the University. This has fostered a substantial number of Web-based services and local uses of information. Unfortunately, it also had made sensitive data vulnerable to compromise such as unauthorized access and/or manipulation. In addition, unsecured systems have recently led to the entire network becoming unusable for the entire campus community.

The risk of compromise is serious and increasing. To minimize exposure, on both the University's behalf and that of individuals, it is critical that computers containing or having access to sensitive data prevent unnecessary and unauthorized access, and that all computers connected to the campus network be secure. They must be managed carefully, thoroughly, and professionally. Until now this responsibility has been left to individual or departmental discretion. The risks have grown substantial enough to require University policy.

In addition to the TTU Code of Computing Practice, the TBR Policy for Information Technology Resources, and other policies previously implemented for TTU, effective from 1 January 2007 forward, computers that contain sensitive data (hereafter called an at-risk computer) may not be connected to the network unless they satisfy security and system-administration requirements, and all systems connected to the campus network meet minimum security requirements.

What Qualifies As An At-Risk Computer?

Computers at risk are those that contain or have automatic access to certain categories of data, especially

1. *student* data covered by the Family Educational Rights and Privacy Act (FERPA),
2. *personnel*, salary, benefits, or other human-resources data, and/or
3. *individual financial* data subject to the safeguarding provisions of the Gramm-Leach-Bliley Act (GLB),
4. *research* data that are the product of Federal or other contracts and grants whose provisions require the University to preserve, maintain, and provide access to those data in the future, or
5. other departmental or *institutional financial* data whose disclosure or loss might impair the University's ability to manage its affairs.

There may also be computers that do not store sensitive data but may be used to access sensitive data on other computers. As a general guideline, if computer A has *automatic* access to sensitive data on at-risk computer B (that is, for example, A's user does not need to enter a username and/or password to see data on B), then computer A is an at-risk computer. If, however, A's user can access sensitive data elsewhere *only by authenticating manually* (that is, entering username and password again), then

computer A is not an at-risk computer. **It is wise to treat any computer that a person regularly uses as an at-risk computer.**

Computers found to contain sensitive data but not to comply with security requirements may be removed from the network by ITS if necessary, without warning. Any computer connected to the campus network and found to pose a security risk to the rest of the campus community may also be removed by ITS if necessary, without warning.

What Is Required Of Computers Connected to the Network?

At-risk computers must adhere to the guidelines in the following five areas, taking appropriate steps to meet the general requirement that it is managed securely and reliably so as to prevent unauthorized access to sensitive data. **All computers connected to the campus network must meet the minimum guidelines listed in item E shown below.**

- A. *Administration.* Computers must be managed to professional standards, by ITS employees or employees with sufficient knowledge and resources to ensure that data on them are properly secured. Operating systems and network-aware applications on computers must be patched and maintained to the most current level provided by their manufacturers.
- B. *Services.* Computers should run no programs or services that are not necessary to their core purpose. For example, computers that contain sensitive data should not run Web or file-sharing services, since these are frequently targeted and compromised by outsiders. Network-aware client software on regulated computers, such as Web browsers or email readers, should block the automatic execution of attachments, graphical files, or other common carriers of computer viruses, Trojans, or worms. Programs known to carry spyware and malware are specifically prohibited. For an updated list of programs currently within this category, please see <http://www.tntech.edu/its/>.
- C. *Users and accounts.* Computers must prevent unauthenticated users from running programs or accessing raw data. For example, there should be no "guest," shared, or general-purpose accounts on regulated computers. Accounts with substantial privileges should be granted only to a few individuals with general management responsibility for the systems in question, and never to individuals without University faculty or staff appointments. The majority of malware and spyware can only execute when the user is logged in as an administrator. System-administrator and similar "root" accounts should be used only when strictly required, and never when use of a less privileged account could achieve the same purpose. The principle of least privilege should be used with few exceptions.
- D. *Access.* User-authentication processes must encrypt or otherwise protect username/password exchanges from interception. User passwords should meet

or exceed ITS's complexity requirements, available at <http://www.tntech.edu/its>. In addition, users with extensive access to at-risk computers should be sure never to use the corresponding passwords for other purposes. All users should avoid recording or writing passwords where they might be discovered.

- E. *Security.* All computers must be reasonably secured against unauthorized access, including data interception and compromise. For example, computers must connect to the network using technologies that are reasonably secure from sniffing, which excludes unencrypted hub or wireless connections. All computers connected to the network must run antivirus and antispyware software, updating definition files frequently. They should also be configured to disable all ports not necessary for system functioning. Furthermore, all computers connected to the campus network must meet a minimum level of functionality regarding processor, memory, and age. Information on the minimum system requirements for connection to the campus network may be obtained from Information Technology Services at <http://www.tntech.edu/its>.

Computers connected to the campus network are subject to random and unannounced security scanning and auditing by ITS and/or the University's internal auditors.

Questions about the specific scope and implementation of these requirements should be directed to ITS at 372-3387.

Proposed by Information Technology Services

Endorsed and approved by Information Technology Committee October 5, 2006

Endorsed and approved by the Administrative Council November 15, 2006