

---

# College of Education Computer Network Security Policy

Learning Technology Center - Technical and Network Services	1/12/2004	-Effective

---

## **Introduction**

The College of Education Network Security Policy provides the operational detail required for the successful implementation of a safe and efficient computer network environment for the College of Education. These security policies were developed based on the understanding of the educational and administrative needs of the College and an evaluation of the existing technical configuration and requirements. These policies are meant to complement existing University of Texas at Austin, University of Texas System, and Texas government policies relating to computer data network security.

---

## **Policies**

---

### **Computer Registration**

All computers which utilize the College's computer data network reserved for faculty, staff, and computer labs must be registered with the College of Education Technical and Network Services. Registration information will include at a minimum the following items:

- Media Access Control (MAC) address of all network interface adapters in the computer.
- Full name of the primary user of the computer. In the case of computers used by multiple individuals, the name and contact information, including email, of the person who is directly responsible for the computer will be provided.

---

### **Centralized Computer Authentication System**

The College of Education will maintain a centralized computer authentication system for computers of the College. All University owned networked computers which are capable of utilizing this authentication system will be configured to verify login credentials with the system. Departments will notify Technical and Network Services of changes to employment status of an employee so that user accounts can be changed or revoked as necessary. Technical and Network Services will maintain documented procedures for departments to notify them of personnel changes.

---

### **Preset Configurations**

All University owned networked computers will have their operating systems and network capable software applications preset with settings approved by the Manager of Technical and Network Services, or designate. These settings will provide a minimum baseline configuration of computers that will ensure computer network security and integrity.

---

# College of Education Computer Network Security Policy

Learning Technology Center - Technical and Network Services	1/12/2004	-Effective

---

## **Administrative Access to All University Owned Computers**

Technical and Network Services will have administrative level access to all University owned computers which are connected to the computer data network reserved for faculty, staff, and computer labs. Technical and Network Services will only utilize this access to a computer under the following conditions:

- At the request of the primary user or administrator of the computer.
- To apply operating system or software application updates or patches to the computer.
- To investigate any suspicious activity by a computer which could lead to network degradation, violate College or University policies, or violate local, state, or federal laws. Use of administrative access by Technical and Network Services to perform an investigation on a computer may only occur with prior approval by one of the following individuals:
  - The primary user or administrator of the computer
  - The director of the Learning Technology Center
  - An associate dean of the College of Education.

Technical and Network Services will inform the designated primary user or administrator of a computer when administrative level access was used by Technical and Network Services to access the computer. A log of the use of administrative access by Technical and Network Services will be maintained and available for review upon request. Technical and Network Services will maintain a list of all personnel authorized to utilize this administrative level access to College computers. The personnel granted this level of access will be full-time senior level Technical and Network Services staff who will all have received training in the proper use of sensitive and confidential information in accordance with College and University policies and all applicable local, state, and federal laws.

---

---

# College of Education Computer Network Security Policy

Learning Technology Center - Technical and Network Services	1/12/2004	-Effective

---

## **Authorized Servers Only**

Technical and Network Services will maintain a list of all computers connected to the computer data network reserved for faculty, staff, and computer labs which are running any network service which is remotely accessible by another computer. Only computers which appear in this list are allowed to run the network services for which they are authorized. Network services must be approved by Technical and Network Services before they will be allowed to run on the College computer data network reserved for faculty, staff, and computer labs. Technical and Network Services will maintain documented procedures for network users to request to run network services on a computer which has not already been approved to run said service. If a previously approved network service on a computer has been found to cause network degradation, violate College or University policies, or violate local, state, or federal laws, the network service authorization for the computer will be revoked.

---

## **Approved Computer Network Device List**

Technical and Network Services will maintain a list of approved network devices which may be attached to the computer data network reserved for faculty, staff, and computer labs. Devices not on this list may not be connected to the College network without prior approval by Technical and Network Services.

---

## **Account Login Information Sharing Prohibited**

Accounts that give users access to Information Resources are to be used only by the persons to whom the accounts are assigned. Log-on Ids, passwords, and other means of access must not be shared with anyone. Holders of means of access are responsible for unauthorized access to their accounts that results from their negligence in maintaining the confidentiality of their means of access.

---

# College of Education Computer Network Security Policy

Learning Technology Center - Technical and Network Services	1/12/2004	-Effective

---

## **Privately Owned Computers**

Computers not owned by the University which are connected to the computer data network reserved for faculty, staff, and computer labs must be configured to ensure reasonable network security and integrity. The computer must be configured but not limited to the following:

- The operating system and software applications on the computer must be updated and patched to eliminate all security vulnerabilities that exist for the computer's configuration.
- An actively running virus scanner which is updated with the latest virus definitions

Privately-owned computers which do not adhere to the minimum standards will not be allowed to connect to the computer data network reserved for faculty, staff, and computer labs. Privately-owned computers which are found to be performing activities which cause network degradation, violate College or University policies, or violate local, state, or federal laws, will not be allowed to connect to the computer data network reserved for faculty, staff, and computer labs.

---

## **Policy Revision Process**

---

### **Changing Environment**

The educational, administrative, technical, policy, and legal environment of the College of Education, as it relates to information technology use and security, is constantly changing. The Network Security Policies will be revised as needed to comply with changes in law or administrative rules or to enhance its effectiveness.

---

### **Technology Neutral**

These policies are technology neutral and apply to all aspects of computer network technology. Emerging technologies or new legislation however, will impact these network policies over time.

---

# College of Education Computer Network Security Policy

Learning Technology Center - Technical and Network Services	1/12/2004	-Effective

---

## **Change Drivers**

A number of factors could result in the need or desire to change the Network Security Policies. These factors include, but are not limited to:

- Review schedule
- New legislation
- Newly discovered security vulnerability
- New technology
- Audit report
- Cost/benefit analysis
- Change in the educational and administrative needs of the College

---

## **Change Process**

Updates to the Network Security Policies, which include establishing new policies, modifying existing policies, or removing policies, can result from three different processes:

- At least annually, the Manager of Technical and Network Services or designate, will review the Policies for possible addition, revision, or deletion. An addition, revision, or deletion is proposed to the College of Education Chairs for approval. If approved by the Chairs, the addition, revision, or deletion will be put into effect.
- Every time new computer network technology is introduced into the College of Education a security assessment must be completed. The result of the security assessment could necessitate changes to the Network Security Policies before the new technology is placed into use in the College of Education computer network.
- Any user may propose the establishment, revision, or deletion of any policy at any time. These proposals should be directed to the Manager of Technical and Network Services or designate who will evaluate the proposal and make recommendations to the Chairs if the proposal is deemed valid and reasonable in accordance with the goals of the Network Security Policy.

---

## **Change Distribution and Notification**

Once a change to the Network Security Policies has been approved by the Chairs, the following steps will be taken as appropriate to properly document and communicate the change:

- The appropriate Network Security web pages will be updated with the change
- Training and compliance materials will be updated to reflect the change
- The changes will be communicated using standard College of Education communications methods such as: email, announcements web page, newsletters, and communications meetings.

---

## College of Education Computer Network Security Policy

Learning Technology Center - Technical and Network Services	1/12/2004	-Effective

---

### **Exception Process**

The College of Education Network Security Policies are likely to be impacted by changing technology, legislation, educational and administrative requirements. The steps for permitting and documenting an exception are:

- A request for an exception is received by the Manager of Technical and Network Services or designate along with a rationale for justifying the exception.
- The Manager of Technical and Network Services or designate analyzes the request and the rationale and determines if the exception should be accepted, denied, or if it requires more investigation
- If more investigation is required the Manager of Technical and Network Services or designate and College of Education computer technical support staff determine if there is a cost effective solution to the problem that does not require an exception
- If there is not an alternate cost effective solution, and the risk is minimal, the exception may be granted
- Each exception must be re-examined according to its assigned schedule. The schedule can vary from 3 months to 12 months depending on the nature of the exception
- Any exception request that is rejected may be appealed to the Chairs.