1. POLICY STATEMENT

All TCS Education System ("TCSES") data stored on a TCSES computer must be stored on the shared network drive assigned to your specific department or to you as an individual. Storing TCSES data on the (network drive will ensure that the data you are working with is backed up and can be restored if necessary. If you need this data outside of the office, you should use the TCSES VPN to connect remotely and perform your work. If that is not feasible, then you may copy the data onto your local hard drive provided that approved technologies are used to encrypt the data. Contact IT for information on the use of approved encryption technologies.

1.1 Laptop Computers

Laptop computers should stay in the possession of the user whenever possible. If the laptop cannot be in the possession of the user, all efforts should be taken to prevent the loss of the laptop and the TCSES information stored within it. For instance, if left in a car, it should be stored out of sight and locked up safely; if left in a hotel room, it should be turned off and out of sight. A laptop computer should never be left logged on and unattended. The laptop should be secured when in use outside the office. This can be accomplished by using a physical laptop cable lock, a secured docking station, placing the laptop in a secured area, etc. Cable locks can be obtained by calling the TCSES IT Help Desk at x 8600.

1.2 Handheld Devices

Mobile phones, iPads and other handheld devices may contain TCSES information in e-mails, attachments, or addresses. They should never be left unattended. Whenever possible the following security features should be enabled on these devices:

- A device password must be enabled
- An auto-lock timeout should be set to no more than 2 minutes

1.3 Lost or Stolen Computing Equipment

If any mobile/wireless computing equipment is lost or stolen, it should immediately be reported to the facility from which it was obtained. The IT Department is then able to "wipe" the information from the device, should that be necessary.

2. PURPOSE

As a component of the TCSES IT Security Program, the purpose of this policy is to maintain the confidentiality, integrity, and availability of the TCSES information assets, and to ensure compliance with legal, contractual, and regulatory requirements.

3. APPLICABILITY

This policy applies to all TCSES employees who use company-issued computing and communication devices (e.g., personal computers, cellular phones, Blackberries, PDAs, etc.) which may contain TCSES information and may be taken out of the office.

4. DEFINITIONS

4.1 Availability

The protection of IT assets from loss and ensuring that they are available to authorized persons or processes whenever and wherever required.

4.2 Confidentiality

The safeguarding of information from access by unauthorized persons or processes.

4.3 Integrity

The completeness and accuracy of information assets.

4.4 IT Security

The provision of organizational, technical, and social measures to preserve the confidentiality, integrity, and availability of IT assets against unauthorized access, damage, or interference, by both malicious and accidental means.