Lost/Stolen IT Equipment Employee Guidelines

Purpose

The College and all of its employees are legally obligated to protect sensitive College data. If this data or the network and computer resources that contain it become compromised or threatened due to the loss or theft of information technology equipment, for example a device such as a laptop or smart phone, the College and its employees must immediately take steps to prevent or minimize the harm or damage that could result.

In the event of a loss, these procedures anticipate the rapid execution of each step-in order to minimize the impact of the loss.

Precautions

If you are a College employee using a college-owned IT device (e.g., laptop, smart phone, iPad, or other), using a personally-owned device to access the College computer network, or storing files with sensitive College data on any device, you must always take the following precautions.

- You are required to have a login password for your device.
- As much as possible, store sensitive College data only on approved College network storage drives rather than on any mobile device or laptop.
- When off-campus using wireless access, use the College's virtual private network (VPN) facilities to access and work on files with sensitive data.
- If you absolutely must put sensitive College data on a device, such as a laptop, the data must be encrypted, and the files must be password protected. When finished using sensitive files, immediately delete them securely from the device.
- Any file with Thiel data that is password protected and encrypted on your hard drive should also be backed up onto a network storage drive.
- Do not allow others to use college-owned devices or learn your Thiel network password. You are solely responsible for actions taken while using your password.
    - If it appears that your password is compromised, such as your e-mail account begins sending out spam, IT will disable your password and notify you to change it.
    - If you know that your password is compromised, you must report it to the IT Help Desk immediately so that it can be reset and changed.
    - If you suspect your password is compromised, you can change it yourself using the Thiel Hub Change Password option. The link for the Thiel Hub can be found on the bottom of the Thiel Homepage. Sign into the Hub and click Change Password under My Account.
- Do not leave your devices unattended. Never leave your devices visible in a parked car. Don't walk away from your devices in a library or other public place, even if "just for a

moment". Don't leave your devices out and visible in your residence if your door is unlocked or you are away.

Report Loss or Theft Immediately to Campus Police

- When equipment or a device (laptop, desktop, smart phone, iPad, other) is lost or stolen on campus, immediately call Campus Police at (724) 589-2222 to report the incident at any time of day or night.
- If a college-owned device or personal device containing Thiel College data or used to access Thiel College data is lost or stolen while off-campus, first file a police report with the appropriate local authorities. Then, also report the occurrence to Thiel Campus Police.
- Campus Police, working with other authorities as applicable, will gather initial details of the loss or theft from you including whether or not the device was on, logged into the College network when stolen, if it contained files with sensitive College data, and if those files were encrypted and password-protected or not. The police will ask for contact information from you for follow-up. Campus Police will immediately contact the IT department.
- The IT department will, among other things, reset your password and block all access to network resources, including e-mail, until such a time that you can change your password.
- IT will contact you to determine the nature and scope of any compromised Thiel College sensitive data.
- If there was a potential compromise of sensitive information or exposure of network resources, the Director of Computer Information Systems may confer with appropriate College officials and/or legal counsel, coordinate notification to affected individuals, and report the incident to state or federal agencies and the media as required.

Related Standards, Policies, and Processes

IT Technology Agreement – Sections 6 and 7

Acceptable Use Policy

IT Security Policy