LMU | Lincoln Memorial University

| **Workplace Device Technologies Standard** | |
|---|---|
| **Version: 3** | **Effective Date: 1/1/2017** |

# Workplace Device Technologies Standard

**Purpose:**
The purpose of this compliance standard is to provide the University community with a clear understanding of the proper practices in the use of various communication technologies available in the workplace.

This standard seeks to ensure that University content is appropriately protected.

**Definitions:**

- **Protected Information is data subject to special precautions in its storage, usage and transmission.**
- **Social Engineering** is the term used for the practice of manipulating people to reveal private or sensitive information as a way to circumvent security.
- **University Data** is all data or information owned, used, created or maintained by the University whether individually controlled or shared, stand-alone or networked.
- **User** includes anyone who accesses and uses the Lincoln Memorial University Information Services resources.

**Standards Statement:**
Lincoln Memorial University provides a communication network offering data, video and voice devices and facilities for use by individuals and groups. The use of communication resources is permitted if users are aware of the information security issues involved and act in compliance with relevant regulations.

**Clear Desk Practice:**

All protected information must be removed from the desk or other public areas and locked in a drawer or file cabinet when the workstation is unattended and at the end of the workday. All protected information must be stored in lockable drawers or cabinets.

File cabinets containing protected information must be locked when not in use or when not attended. Keys used to access protected information must not be left at an unattended work area.

**Providing Services or Instruction by Telephone:**

Instruction and service information is routinely provided by University employees by telephone. The University prohibits the release of private information. Be aware of the all relevant policies and procedures when sharing information by telephone. Use a verification procedure to assist in determining the identity of the caller. Be aware of techniques, such as social engineering, used to gain information by deception.

**Recording Telephone Conversations:**

Federal and state laws require that all parties must be informed in advance if calls are recorded. Quality assurance calls should identify that monitoring used to improve training. Recorded material must be safeguarded from unauthorized access and disclosure.

**Clear Screen Practice:**

Computers and displays should be logged off or protected by a screen and keyboard locking mechanism controlled by a password or similar user authentication mechanism when unattended or protected by key locks, passwords or other controls when not in use. Users should shut down their computers at the end of the workday. Passwords must not be posted on or under a computer or in any other accessible location.

**Printers and Facsimile Transmissions:**

Prevent the unauthorized use of photocopiers, facsimiles, multifunctional and other reproduction technology. Designate a responsible individual to handle secure photocopies and faxed communications. Copies of documents containing protected information must be immediately removed from printers and facsimile machines. Consider using printers with pin code functionality to limit access to only those who originate the document. To the extent possible, isolate the devices to a secure location accessible only to authorized employees.

For facsimile transmissions, use cover sheets that clearly identify the intended recipient and the total number of pages faxed. Use caution when sending or receiving confidential information by fax by confirming the number before dialing, requesting confirmation and reviewing activity reports. Confidential communications should explicitly state that the fax should not be distributed, copied or disclosed to any unauthorized person. Instructions on the handling of facsimile communications received in error should be provided on the cover sheet.

**Removable Storage Media:**

All protected information should be locked away from the workstation when not required and at the end of the workday. All protected information must be stored in lockable drawers or cabinets.

**Mobile Phones:**

Mobile phones are not secure and can be easily monitored. Do not convey sensitive or confidential information on a mobile phone. Mobile telephones should be secured with a PIN to protect address and telephone data.

**Conference Calls/Videoconferencing:**

Use caution when discussing sensitive content. Public communication lines can be compromised. If conference calls or videoconferences are required on a regular basis, or if confidential data is discussed; use appropriate encryption on the lines. It is important to establish a procedure to verify the identities of the parties participating in a conference call.

## Inquiries:

Direct inquiries regarding this policy to:

**Office Locations & Address**

Lincoln Memorial University
Information Services, Duke Hall
6965 Cumberland Gap Parkway
Harrogate, TN 37752

## Mailing Address:

Lincoln Memorial University
Information Services, Duke Hall
6965 Cumberland Gap Parkway
Harrogate, TN 37752