Background

The purpose of this policy is to ensure all IT@UC employees lock their workstations whenever unattended; left in an accessible mode, a computer is vulnerable to a wide variety of attacks including theft of the computer and theft of information contained on or located by the computer. Locking the computer strongly mitigates the risk posed by these attacks.

Policy

All personnel must physically lock their laptops.

All personnel must logically lock their laptops or desktop computers when those computers are unattended, even for just a few minutes.

A representative of the University’s Office of Information Security will conduct random audits to enforce this policy.

If a computer is found unattended and not locked during an audit, that computer will be locked and details of the violation recorded. If a computer is found to be unlocked while unattended three times, administrative discipline may be taken.

1. **First violation**: Violation will be recorded, the computer will be locked and a reminder of the policy will be provided to the employee.

2. **Second violation**: Violation will be recorded, the computer will be locked using a Security account which will require the user to contact the IT@UC Helpdesk (556-4357) to unlock, and a reminder of the policy will be provided to the employee.

3. **Third violation within 12 months**: Violation will be recorded, the computer will be locked using a Security account which will require the user to contact the IT@UC Helpdesk (556-4357) to unlock, a reminder of the policy will be provided to the employee and the matter will be referred to management for administrative discipline.

Audience:

This policy applies to all organizations and individuals associated with the University of Cincinnati Department of Information Technology.
Disciplinary Actions:

Violation of this policy may result in administrative discipline.

Definitions:

Audit: An audit will consist of a manual review of random UCit work areas by a UC Information Security designee to ensure that all unattended computers are locked or shut down.

References:

ISO 27001/17799, International Standards Organization for Information Security
COBIT 5.0, ISACA Audit Controls Objective
Payment Card Industry (PCI), Credit card processing and usage compliance requirements

Related links:

- International Standards Organization 17799:2005
- Control Objectives for IT

Contact Information:

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

History:

Issued: 02/01/2010
Revised: 2/15/2015
Appendix A

*Locking your computer*

- A computer running Microsoft Windows may be locked by either of these methods:
  1. Pressing the **windows key** + L
  2. Pressing **Ctrl + Alt + Del**, then **Enter**

- A Mac computer may be locked by either of these methods:
  1. Enable the *security password upon waking up* from either sleep mode or screen saver mode. This option may be enabled under **System Preferences → Security → General**.
  2. Enable *fast user switching* inside **System Preferences → Accounts → Login Options**. The system can then be locked by clicking on the icon on the menu bar and choosing Login Window....