**ITSC 1325**

**Personal Computer Hardware**

**Course Content Lead:** xxxxxxxxxxx

**What is the end goal of this course?**  Install, configure, secure, and troubleshoot operating systems software and hardware to achieve high availability and performance.

**PSLO Information:**

Introduce PSLO 1: (Network Design & Implementation) Student will demonstrate knowledge and expertise of network components, protocols, services, and operation, by designing and implementing a functional network (hardware, software, services), given business requirements and constraints

Introduce PSLO 2: (Network Security) Student will demonstrate expertise in configuring a secure IT infrastructure

**WECM Course Information:**

**Please note:** Course information is included as a resource and is not meant to be utilized as a course outline. Course Categories/Topics and individual KSAs (Knowledge, Skills & Abilities) should come from industry and be itemized. With the general nature of Course outcomes, it should be very easy to ensure that End of Course Outcomes are met and mapping will be done in the future to ensure that there are not any gaps. Please utilize this opportunity to take a look at each course with fresh eyes and carefully consider industry needs and the needs of your program as you go through the deconstruction process. Please do not hesitate to contact xxxxxxxxx (xxxxxxxxxx@tstc.edu) if you have any questions or need any assistance

[**Course Info**](http://board.thecb.state.tx.us/apps/wecm/PubDispRegular.cfm?CRSID=4486)

**Course Level:** Introductory

**Course Description:** Current personal computer hardware including assembly, upgrading, setup, configuration, and troubleshooting.

**Course Outcomes:**

**CO1:** Assemble/setup personal computer systems

**CO2:** Upgrade personal computer systems

**CO3:** Diagnose and isolate faulty components

**CO4:** Optimize system performance

**CO5:** Install/connect peripherals

**Added Outcomes:**

**CO6:** Document baseline configuration and system component upgrades

**CO7**: Secure desktop environment

**CO8**: Customize a PC for an end user

**(Domain) Units/Categories**

**1. Computer Components**

**2. OS Installation**

**3. Windows Performance Monitoring**

**4. PC Troubleshooting**

**5. PC System Security**

**6. Thinking Outside the Box**

**5. End User System Security** [CO7, CO8]

**CC 5.1 Secure a personal computer system  
LO 5.1.1 Identify system secure vulnerabilities  
LO 5.1.2 Implement security best practices to harden a workstation**

**LO 5.1.1 Identify system secure vulnerabilities**

1. User Security Awareness
   1. Unauthorized Access
      1. Administrative Access
      2. Dumpster Diving
      3. Shoulder Surfing
   2. Social Engineering
      1. Telephone Scam
      2. Phishing
   3. Data Destruction
   4. Physical System Crash / Hardware Failure
   5. Physical Theft
   6. Shut down System
      1. Minimum Password Length
      2. Account Lockout Threshold
      3. Disable Windows Installer
      4. Printer Browsing
   7. Virus and Threat Protection Software
      1. Anti-Malware
      2. Antivirus
         1. Definition File
      3. Virus Shield
         1. Signature
         2. Checksum
      4. Careful Clicking
      5. Recovery
         1. Recognize and Quarantine
         2. Search and Destroy
         3. Remediate

**LO 5.1.2 Implement security best practices to harden a workstation**

1. Device Hardening
   1. Hardware
      1. Set BIOS password
      2. Disable Autoplay for removable media
   2. Software
      1. Genuine Licensed OS
      2. Genuine Application software
      3. Encryption
         1. BitLocker
      4. Secure web browsers
      5. OS Lock on Timeout
      6. Uninstall inactive apps and features
      7. Disable unnecessary services
      8. Set Privacy Controls
         1. Location
         2. Camera
         3. Microphones
      9. Windows Firewall and Protection
         1. Private Network
         2. Public Network
         3. Allow Applications
            1. TeamViewer
      10. Parental Controls
          1. Web sites
          2. Time restrictions
          3. Reporting
          4. Apps and Games
   3. Mobile Device
      1. Patches/Updates to OS
      2. Find my iPhone
      3. Passcode Lock
      4. Remote Wipe
      5. Touch ID
      6. Backups
      7. App Permissions

|  |  |  |  |
| --- | --- | --- | --- |
| **Resources**  **(This table is for ALL instructors to share resources. Right click to add rows as necessary)** | | | |
| **Current/Planned Resources & Materials**  Videos, Books, Simulations, etc. (Be Specific, include chapters, links, vendor info) | **Assignments**  Practice Labs, Quizlets, and Interactive Activities | **Tests and Major Projects**  Tests/Exams, Projects  What are the planned summative assessments?  Projects (-Performance Assessment- Hands on) and Tests/Exams  (OA- Objective Assessment- Test, Quizzes) | **Proposed New Material and Content**  Are there any major materials that you are thinking of adding that would need to be developed?  Workbooks, Simulations, etc. |
| **LO 5.1.1 Identify system secure vulnerabilities** | | | |
| Slides 5.1.1 System Vulnerabilities | Quiz- System Vulnerabilities |  |  |
| **LO 5.1.2 Use security best practices to harden a workstation** | | | |
| Slices 5.1.2 PC Hardening | Lab - PC Hardening |  |  |
| MasteryAssessment |  | OA - PC Security [Multiple Choice, Matching, Essay] |  |
| **Comments/Notes** |  | | |