I. PURPOSE
The purpose of this Standard is to ensure that all employee owned electronic computing devices and/or electronic storage media are configured and used appropriately when accessing university resources.

II. SCOPE
This Standard applies to all University and Auxiliary:
- faculty, staff, students, and volunteers (collectively referred to as “employees”), contractors and consultants,
- computing devices and/or electronic storage media with access to campus resources.

III. STANDARDS

A. Storage of Confidential/Internal Use Content on Computing Devices/Electronic Storage Media
Level 1-Confidential and Level 2-Internal Use information (refer to Information Classification Standard) must be stored on University owned and secured databases or file servers. When access to a secure server is not available and when approved by the employee’s Appropriate Administrator, Level 1-Confidential and Level 2-Internal Use information may be stored on University owned laptops, desktops or electronic storage media. Such laptops, desktops and electronic storage media must be encrypted or otherwise rendered unreadable and unusable by unauthorized persons and must be located in a secure location at the University or another site approved by ITS and/or OAT management (including off-site backup services) in accordance with the CSULB Electronic Data Security – Portable Devices and Removable Media Standard.

Level 1 and Level 2 information may not be stored on non-university/auxiliary owned equipment including but not limited to laptop computers, desktop computers, electronic storage media, personal digital assistants (PDAs), or cell phones (such as BlackBerry®, Treo®, and iPhones®).

B. Accessing Confidential/Internal Use Content with a Computing Device
All employee owned electronic computing devices accessing university resources shall meet the following minimum standards:
- Maintain a currently patched/updated operating system.
  - Patches and updates are available from the respective operating system vendors and should be applied, either automatically or manually, as soon as possible after they are released.
- Current anti-virus software installed, activated, and regularly updated.
  - Software should be from a recognized vendor such as McAfee, Microsoft, Sophos, Symantec, etc.
- Periodically scan electronic computing devices to detect malware.
- Use strong passwords (refer to CSULB Password Standard)
- Regularly update all software with security patches.
- Delete cookies, history, and temporary files upon exiting the internet browser software.
C. Use of E-mail to Transfer Confidential/Internal Use Content

Level 1-Confidential information may only be transferred by email to those employees with an established business need-to-know and are either CSULB employees or someone who has signed a confidentiality agreement. Email may be sent within the CSULB email system (@csulb.edu) but not over a public network unless password protected or encrypted. All email transmissions of confidential information must contain the following statement: “The information contained in this email message or its attachment is confidential. Dissemination or copying of this email is strictly prohibited. If you think that you have received this email in error, please email the sender.”

Level 2-Internal Use information may only be transferred by email to CSULB employees and those individuals with a business need-to-know. Email may be sent within the CSULB email system (@csulb.edu) or over a public network to persons with a business need-to-know.

IV. DEFINITIONS

| Electronic Computing Devices | Include, but not limited to, desktop computers, laptop computers, PDAs, tablet PCs, and smart phones. |
| Electronic Storage Media     | Include, but not limited to, CD-ROMs, DVD-ROMs, external hard drives, zip disks, floppy disks, reel and cassette format magnetic tapes, flash-memory cards, magnetic cards and USB flash drives (a.k.a. Memory Sticks, Thumb or Jump Drives). |
| Encryption                  | The process of altering electronic information using a code or mathematical algorithm so as to be unintelligible to unauthorized readers. Encryption software and assistance can be obtained through area Information Technology Coordinators or through Information Technology Services. |
| Malware                     | Short for "malicious software," malware refers to software programs designed to damage or perform other unwanted actions on a computer system. Common examples of malware include viruses, worms, trojan horses, and spyware. |
| Operating System            | Also known as an "OS," this is the software that communicates with computer hardware on the most basic level. Without an operating system, no software programs can run. The OS is what allocates memory, processes tasks, accesses disks and peripherals, and serves as the user interface. Examples of operating systems include Microsoft Windows, Apple Macintosh (Mac), and Linux. |
| Software                    | Computer software is a general term that describes computer programs. Related terms such as software programs, applications, scripts, and instruction sets all fall under the category of computer software. Therefore, installing new programs or applications on your computer is synonymous with installing new software on your computer. Examples of software include Microsoft Word, Microsoft Excel, Adobe Acrobat, etc. |

FURTHER INFORMATION
Information Security Management and Compliance
iso@csulb.edu.
(562) 985-4862