Policy/Procedure Regarding Securing Laptop Computers, Portable Media, and Sensitive Data

Training

Each laptop user, regardless of whether the laptop has been/is being allocated on a permanent or temporary basis will be required to take the "Information Security and Mobile Devices" online training course and provide evidence of successful completion.

Security

Whenever a CCSU computing device or storage media, including but not limited to laptop computers and/or external storage media such as a USB memory stick, portable hard drives, CDs, DVDs, floppy disks or tapes, is found missing, stolen or lost, the individual responsible for the device or media will report the loss to his or her supervisor and the office of the Chief Information Officer within one hour of ascertaining the loss. In keeping with current policy and procedure already in effect, notice is also to be made to the campus police department as a loss/theft of state property.

Sensitive Data Control

Sensitive data, including but not limited to SSN, driver's license number, credit card number, bank account number, tax information, date and/or location of birth, and all such personally identifiable information as specified under FERPA, will not be stored on portable computing devices or media (as described in "Security" section). Data residing on CCSU servers should be accessed via the use of existing Virtual Private Network (VPN) and Citrix technologies when off campus.

Requests for Policy Exception

Any employee/department that feels they have compelling need to store such data on a portable computing device will 1) document the reason(s) justifying the need and 2) forward the document with a request for an exemption to the Chief Information Officer, via the divisional Executive Committee member, who will perform, or arrange to perform, a documented risk assessment and make a recommendation to allow or disallow the exemption. The exemption request, risk assessment, and the recommendation will be presented to the President, or his/her designee, for final determination as to whether the exemption will be granted or not.

If the exemption is granted, the exempted user is responsible for ensuring that an acceptable encryption software/device is employed to further safeguard the information. The office of the Chief Information Officer will provide timely suggested alternatives to meeting this requirement.

In all instances, the use of the Virtual Private Network (VPN) and/or Citrix technologies to connect to university servers via the internet is preferable to copying/storing information on portable computing devices and media when working off campus. Any questions regarding alternative solutions to storing sensitive data on a portable computing device should be directed to the Chief Information Officer.
November 17, 2009