Western Connecticut State University (WCSU)
Laptop Policy Effective 1/1/08

Note: As a result of recent computer thefts in the state and at our university, University Computing will be recalling all university-owned laptops to gather additional information and apply security updates.

General guidelines/tips to better protect university equipment from theft:

- Always lock your office when you leave. It only takes a second to steal your laptop.
- Always lock your computer system when you step away from your office or desk.
- Change your password often and make it hard to guess.
- Always lock the classroom door(s) when your class is over.
- Require students for the next class to wait until the next professor arrives to open the room.
- Do not leave equipment unattended whether on campus or off-campus i.e., never leave your laptop in your car or in visible site.
- When traveling, keep your laptop with you at all times.
- Report any suspicious activity or people to the University Police immediately. Try to make note of details to be able to provide a good description of the individuals.
- Use discretion with student grades and DEC evaluations. Never store them on the hard drive of the laptop.

Security Notice to All WCSU Employees:
New Procedures Regarding Securing Laptops, Portable Media and Sensitive Data – EFFECTIVE 1/1/08

Whenever a WCSU computing device or storage media, including but not limited to laptop computers, is found missing, stolen or lost, the individual responsible for the device or media will report the loss to his or her supervisor, University Police and the Chief Information Officer within one hour of ascertaining the loss. Paperwork will subsequently be filed with the Associate Director of Property Management to appropriately track the asset.

Sensitive data (e.g., SSN, driver's license number, credit card number, bank account/routing number, tax information (TIN, EIN, Student/Parent salary info), State Employee ID, International documents (Visa, etc.), PIN, date and location of birth, and all such personally identifiable information as specified under FERPA) will not be stored on portable media (e.g., laptops, USB stick drives or thumb drives, portable hard drives, CDs, DVDs, tapes, smartphones.) If there is a compelling business need, the Chief Information Officer or designee will conduct a documented risk analysis. The business case and risk assessment will then be presented to the President or his designee for review and authorization. If a compelling business need is authorized, if feasible, sensitive data stored on portable media will be encrypted with a WCSU-approved encryption method. Encryption of the entire drive will be evaluated and implemented as soon as possible.

I understand the above responsibilities and accept them.

Signature:_____Date:_____

Printed Name:_____Dept._____