NVCC Security Policies and Procedures
On Storage of Sensitive Data and Portable Storage Devices

(Approved by Administrative Council 1/22/2008)
Revised 2/10/2009

Storage of Sensitive Data and Information

Sensitive information should only be stored within secure network applications such as PeopleSoft, BlackBoard, and the NOVA HR System or on an individual's network drive which is located on a college server. Sensitive information should not be stored on portable storage devices, individual desktop computers, personal web pages/sites, or home computers. Sensitive data/information is any data where the unauthorized access, loss, misuse, modification, or improper disclosure could negatively impact the ability of the college to provide benefits and services to its students or could compromise the privacy of an individual's records. This includes, but is not limited to, personally identifiable information outside the scope of the college's directory information policies; social security numbers; personal financial information; sensitive plans and procedures; personnel records; individual student records; and student grades. Any storage of sensitive data/information other than on a network application or network drive must be approved in advance by the Vice President for Instructional & Information Technology and should only be done on devices provided by the College. Any loss of sensitive information should be reported immediately to the Vice President of Instructional & Information Technology.

Portable Storage Devices

Sharing files, copying and moving files, and flexibility with respect to digital information is essential to the instructional process, as well as for disaster recovery and continuity of operations. The College is willing to assume the risk associated with the use of portable storage devices (such as usb drives, laptops, CD-R, DVD-R, floppy disks, etc.), and will rely on our antivirus software and other network safeguards to protect our network and digital information.

To provide further protection of the College's network and sensitive information without interfering with the instructional process and academic freedom, the use of portable storage devices—usb drives, laptops, CD-R, DVD-R, and floppy disks—must be limited to data that can be made public (in case they are lost or stolen). **Private, sensitive data should never be stored on these devices—especially identifiable personal data like social security numbers, emplids, student grades, etc.** This applies to any of these devices—even personally owned ones. Any of these devices that are owned by the college (especially laptops), connected to a college computer, or connected to the college network should use ITSS approved encryption software to protect all document/data files on these types of devices to prevent them from being compromised if the device is lost or stolen. In the limited cases where potentially sensitive data that should not be made public must be stored on a portable device (such as for disaster recovery or continuity of operations), ITSS approved encryption software must always be used

In the rare event where sensitive data must be stored outside a network application or network drive, the following information is required to process approval of an exception: business or technical justification, scope of data, duration (not to exceed one year), description of potential risks, steps to protect the data.