Storage of Sensitive Data and Portable Storage Devices

Policy Number: 504

Categorized: Information Technology

Responsible Office: VP of Instructional and Information Technology

Subject: Policy and procedures governing the use of portable storage devices and the security of sensitive data

Related Policies: Acceptable Computer Use Policy

Procedures: See below.

Additional Information:

Effective Date: 01/22/2008

Last Reviewed Date: 05/25/2020

---

1. Scope

This policy applies to all Northern Virginia Community College (NOVA) employees, including full and part-time staff, faculty, contractors, consultants, volunteers, interns, student hires, and students (collectively, “users”).

2. Policy Statement

Sensitive information should only be stored within secure network applications such as PeopleSoft, Canvas, 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. Any loss of sensitive information should be reported immediately to the Vice President of Instructional & Information Technology.

In the rare event where sensitive data must be stored outside a network application or network drive, it must be approved in advance by the Vice President of Instructional and Information Technology.

3. Definitions

Portable storage devices: usb drives, laptops, CD-R, DVD-R, and other external storage.

Sensitive data/information: 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.

4. Procedures

a. Limitations on Use of Portable Storage Devices

   i. The use of portable storage devices – USB drives, laptops, CD-R, DVD-R, and other external storage—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.

b. Use of Encryption Software

   i. Any portable storage 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.

   ii. 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.

c. Violations

   i. Violations of this policy will be addressed under DHRM Policy 1.60, Standards of Conduct, or VCCS disciplinary policy or procedures for employees not covered by the Virginia Personnel Act. The appropriate level of disciplinary action will be determined on a case-by-case basis, with sanctions up to or including termination depending on the severity of the offense, consistent with Policy 1.60 or VCCS policy.

5. Authority

DHRM Policy 1.60 Standards of Conduct

NOVA Administrative Council (January 22, 2008)

VCCS IT Security Standard and Policy