Storage of Sensitive Data and Portable Storage Devices Procedure

Procedure Number: 504P

Responsible Office: VP of Information and Engineering Technologies (IET) and College Computing

Forms: N/A

Effective Date: 03/08/2024

Date Last Reviewed: 03/08/2024

---

1. Purpose

This policy procedure details the specific actions to be taken by all Northern Virginia Community College (NOVA) employees, including full and part-time staff, faculty, contractors, consultants, volunteers, interns and student hires, and students (collectively "users") who use portable storage devices.

2. Definitions

Portable Storage Devices: include 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 NOVA 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 (PII) outside the scope of NOVA's directory information policies; social security numbers; personal financial information; sensitive plans and procedures; personnel records; individual student records; and student grades.

3. Procedure

1. Limitations on Use of Portable Storage Devices

   a. 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.

2. Use of Encryption Software

   a. 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 Information Technology Support Services (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.

   b. 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.

3. Violations

    a. Violations of this policy will be addressed under the Virginia Department of Human Resource Management (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 of employment depending on the severity of the offense, consistent with Policy 1.60 or VCCS policy.