New River Community College
Sensitive Data

Sensitive Data/Information

The term *Sensitive Data/Information* refers to critical information for which the unauthorized access, loss, misuse, modification, or improper disclosure could negatively impact the ability of the VCCS Entity to provide services and benefits to its students. Examples of Sensitive Data with regard to disclosure of Personally Identifiable Information includes the first name or first initial and last name in combination with and linked to any one or more of the following data elements, when the data elements are neither encrypted nor redacted.

The term *Encrypted* means to encode the data in such a manner as to render it unreadable without an encryption key, as defined by accepted encryption standards.

The term *Redact* means to alter or truncate data such that no more than parts of the following information is accessible.

Sensitive Items

1. Social security number
2. Driver’s license number or state identification card number issued in lieu of a driver’s license number.
3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial accounts.
4. Other personal identifying information, such as insurance data or date of birth.
5. Five digits of a social security number; or
6. The last four digits of a driver’s license number, state identification card number, or account number.

Note: The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public

All agency systems, processes, logical and physical data storage locations that contain personally identifiable information are considered sensitive, raising the standard of compliance to the standard of compliance for systems containing sensitive data.

Storage of these items on Commonwealth of Virginia and NRCC systems is not permitted unless it is specifically required for college business. Normal college business operations require that sensitive information be maintained in many departments. If your department is required to store sensitive information as defined in the next section, you as the data owner, are responsible for notification of Information and Educational Technologies of the need to store sensitive information and to classify your data storage requirements as defined in the college's Continuation of Operations and Disaster Recovery Plans.

Sensitive data is never to be stored on portable storage devices in unencrypted form, including laptop computers, CD/DVDs, USB Keys, cell phones or PDAs. In the event that there is a business requirement to store sensitive data on a portable device, documentation of the nature of the data and justification for storing it on portable media must be submitted in writing to the College Chief Information Security Office along with documentation of processes that will be used to secure this data. Information and Educational Technologies will work with the data owner to establish storage that is compliant with the applicable state, VCCS and college guidelines.

Secure Transmission of Sensitive Data

Sensitive data must be protected from exposure to unauthorized persons or when it is exchanged with authorized recipients outside the normal security boundaries of the VCCS network. Authorized recipients may include other VCCS employees, consultants, cloud services providers, or other entities with approved non-disclosure and acceptable use agreements on file.

Transmission of sensitive data using email is not allowed unless the data is included as an encrypted attachment or the email itself sent encrypted. Note that some email servers will reject or strip off unrecognized attachments, so this method is not always reliable. Send the encryption key (password) to the recipient using an alternate communication method (cell phone) to ensure the data and the encryption key are transmitted separately.