COLUMBUS STATE
INSTITUTIONAL REVIEW BOARD

# Research Data Security and Disposal

## SECURITY

Keeping data confidential and secure is important in all research projects. The IRB has these common concerns with data storage. The Principal Investigator (PI) must address them, as appropriate, in an exempt protocol abstract or an expedited or full protocol narrative.

**Steps to ensure research data is secure:**

- *Anonymize the content:* for example, replace participant names with non-personally identifiable descriptors; code demographic, behavioral patterns and other types of responses
- *Control access:* limit access to data to the PI and other members of the research team as designated on the protocol form
- *Encrypting files:* this is one of the most common and effective methods to achieve data security and also allows for the safe transfer of information
- *Backups and copies:* ensure they are controlled and secure
- *Consider exactly what is needed:* only keep what is needed; don't be tempted to hold on to data "just in case"

**Paper consent forms and surveys:** These should be kept in a locked file within a locked office.

**Online surveys:** At Columbus State online surveys are developed using SNAP, a secure software. Submit requests for SNAP survey development through the Office of Institutional Effectiveness ticketing system at Make a Request (survey request type).

When establishing a survey on Zoomerang, SurveyMonkey, or other online sites, the PI must determine how the survey site protects data. All survey sites can provide a security certificate that indicates how confidentiality is protected. *Provide a copy of this document with the protocol.*

**Data collection on a PC or laptop:** Personal computers can be hacked into, laptops can be stolen, and flash drives can be lost. Encrypting of data is encouraged so that only the PI can read it. Encryption software such as BitLocker or VeraCrypt are available. *In the protocol, indicate how any computer-stored data will be secured.*

## DISPOSAL

Federal regulations require that research data and consent forms shall be retained for three years after the completion of the research. *The protocol should state how data will be destroyed at the end of that time.*

Options include shredding paper documents. Data on hard drives can be deleted with utilities such as Eraser and File Shredder. To find software, search online for "free secure file deletion". Flash drives can be cleared using a right click of the mouse and choosing to delete.