

## Data Security

Gone are the days of research data being exclusively obtained through the use of paper and pencil survey instruments. With ever-growing technology from shared drives, cloud-based programs and internet data collection, the need for researchers to safeguard their records for the privacy of human subjects has expanded to new horizons. Researchers are federally required to provide a plan for protecting the confidentiality of their research data when it is collected, stored, transmitted or shared.



It is imperative that FAU researchers work with their department, college and university technology experts to receive guidance as to the best way to secure and safeguard research data.



*Each college has their own IT staff who can help develop data security and safety monitoring plans. Contact your IT personnel to learn more.*

The first step in creating a data safety monitoring plan is to gauge the level of security that is necessary based on the sensitivity of the data. The more sensitive the information, the higher the level of security measures that must be taken.

Some tips for data security practices at any level include:

1. Collect the minimal amount of identifiable information necessary for the study
2. Change access passwords at least once every 90 days
3. Lock or log off computers when leaving your station for any measure of time
4. Protect your computer with antivirus and spyware programs
5. Encrypt! Encrypt! Encrypt files on your computer and especially before transmitting them to authorized others

For more helpful measures click [here](#) to see FAU's Information Access and Security Policy.

