08:16:06 DATA SECURITY

1. In simple terms, data security is the practice of keeping data protected from corruption and unauthorized access.

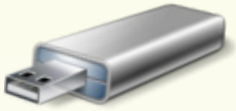
2. All data is to be secured, managed, retained, and disposed of per ChSCC, TBR, State and Federal guidelines. The decision on handling and classification is determined from 3 separate areas:

- Identification
- Integrity
- Availability

If you're not sure what actions are right, read the complete policy ChSCC 08:16:06 Data Security and also review the referenced documents.

3. Everyone that has access to ChSCC data is expected to know and implement the requirements for data security based on the type of data being accessed. Data access is classified either Public data or Confidential.

This includes:



- Any type of data medium (paper, tape, hard drive, email, hard copy documents, electronic – such as phone and iPads, fiche, cloud, etc.)
- Any form (text, graphics, video, web, voice, etc.)
- Any type of computer device provided by ChSCC or your personal device if used for ChSCC business.

4. Access to data is granted based on job requirements defined by the supervisor or through specific processes, e.g., Banner access process authorized by the data owner.

5. Always secure your desktop when you have to leave your office by either locking your keyboard and/or locking your office door.

Security is everyone's job at ChSCC. For full guidance on this and all other Technology policies please go to the Technology web site at:

technology.chattanoogastate.edu/policies-procedures

Chattanooga State Community College