Data Classification and Storage Table

Data at CSU falls into three classifications: Public, Restricted and Private. These classifications are determined by the sensitivity of the data involved and affect how the data should be stored and transmitted. Because of differences in the confidentiality, integrity and availability requirements of these data types, and the confidentiality, integrity and availability of storage and transmission tools, care must be taken in choosing the appropriate tools per data type. This list is not exhaustive but provides general guidelines regarding where to store and how to transmit different types of data.

What	Where
Public: Data explicitly made available to the public. For example: - Directory data, social media, blogs/press releases, published data	University computers/devices (unencrypted) OneDrive Non-university computers/devices (subject to Acceptable Use Policy) Outlook email
Restricted: Data used only within the confines of the University; specific and appropriate approval needed for sharing - All institutional data that does not qualify as public or private should be considered Restricted	University computers/devices (unencrypted, password-protected) OneDrive (with permissions set appropriately) Rstor Outlook email (with permissions set)
Private: Most sensitive, access and approval required by the appropriate Data Authority and must not be shared outside the University. For example: - Personally Identifiable Information, proprietary research information, federally regulated information* - FERPA, HIPAA, human subjects data Note: Additional considerations, such as locking computer screens when not in use, managing access to files and folders, use of strong passwords and Multifactor Authentication, as well as sanitizing devices before disposal will also apply *CUI, ITAR, Classified data and other highly regulated data types will require more stringent measures not listed here	University computers/devices (encrypted and password-protected) OneDrive (with permissions set appropriately) REDCap** Outlook email (encrypted)*** **Available for specific use cases only ***CUI, ITAR, Classified data and other highly regulated data types will require more stringent measures not listed here

Reach out to your department IT, Division of IT or Sarah Robinson with the Cybersecurity Services Team (sarah.robinson@colostate.edu) if you have any questions or concerns.

COLORADO STATE UNIVERSITY