USU DATA STORAGE QUICK REFERENCE

STORAGE*	Restricted Data			Confidential Data	Public Data	Research Data	
	sPII	HIPAA	PCI			Subject to Export Controls	Research Containing Sensitive Data
Local Machines**	X	X	X	✓	✓	X	✔
Employee Personal Devices**	X	X	X	✓	✓	X	X
Unencrypted Portable Storage Devices (e.g., USB drives)	X	X	X	X	✓	X	X
Box (USU Accounts)	✓	✓	X	✓	✓	X	✓
Aggie Shares	X	X	X	✓	✓	X	✓
Local Storage on Dedicated Server*	✔	X	X	✓	✓	✔	✔
Storage with third-party SaaS	✔	✔	✔	✔	✓	X	✔
Google Drive/Apps (USU Accounts)	X	X	X	✓	✓	X	✔
Microsoft OneDrive/Office365 (usu.edu G-Suite and aggiemail.usu.edu G-Suite)	X	X	X	✓	✓	X	✔
ServiceNow	✓	X	X	✓	✓	X	✔
Dropbox	X	X	X	X	✓	X	X
Digital Commons (Library Repository)	X	X	X	X	✓	X	X
Qualtrics	X	X	X	✔	✓	X	✔
RedCap	✓	✓	X	✓	✓	✔	✓

* Storage can be used to store, process, or transmit the classified data types as long as the storage complies with University policies, federal regulation, and contractual agreements. Storage locations apply to USU accounts, not personal accounts.

** Local Machines and Personal Devices can be used to interact with data on approved designated network; however, they are not considered long-term storage devices. Devices accessing Restricted Data must meet USU's required computer security standards.

✔ To Be Determined based upon contractual and data sharing agreements.
Highly sensitive research data (e.g. vulnerable populations) require additional safeguards, e.g., encryption.